Policy Recommendations for Decentralized Finance (DeFi)

Consultation Report

THE BOARD
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

CR/04/2023	September 2023

This paper is for public consultation purposes only. It has not been approved for any other purpose by the IOSCO Board or any of its members.

Copies of publications are available from:
The International Organization of Securities Commissions website: *www.iosco.org*

Foreword

The International Organization of Securities Commissions (IOSCO) has published this Consultation Report with the aim of finalising IOSCO's policy recommendations to address market integrity and investor protection issues in decentralized finance (DeFi) by the end of 2023.[1] In line with IOSCO's established approach for securities regulation, the Policy Recommendations for DeFi[2] are addressed to relevant authorities and look to support jurisdictions seeking to establish compliant markets in the most effective way possible.

Feedback to the Consultation Process

IOSCO welcomes input from all stakeholders as part of this consultation process.
Please submit consultation responses to deficonsultation@iosco.org on or before 19 October 2023.

Your comment letter should indicate prominently that it is a *Public Comment on IOSCO's Consultation Report on Policy Recommendations for Decentralized Finance (DeFi).*
All comments received will be made available publicly unless anonymity is specifically requested. Comments will be converted to PDF format and posted on the IOSCO website.

Following the public consultation period, IOSCO aims to finalize the DeFi recommendations and publish a final report around the end of 2023, in accordance with its Crypto-Asset Roadmap of July 2022, and in conjunction with its CDA recommendations.

[1] The DeFi Working Group is led by staff from the United States Securities and Exchange Commission, with members from the staff of the Australian Securities and Investments Commission; Securities Commission of The Bahamas; European Securities and Markets Authority; French Autorité des Marchés Financiers; Hong Kong Securities and Futures Commission; Central Bank of Ireland; Italian Commissione Nazionale per le Società e la Borsa; Financial Services Commission/Financial Supervisory Service of the Republic of Korea; Mauritius Financial Services Commission; Ontario Securities Commission; Quebec Autorité des Marchés Financiers; Monetary Authority of Singapore; Comisión Nacional del Mercado de Valores of Spain; Financial Conduct Authority of the United Kingdom; and the United States Commodity Futures Trading Commission.

[2] The Policy Recommendations in this Consultation Report are focused on decentralized finance (DeFi). IOSCO has separately consulted on issues related to Crypto and Digital Asset Markets more generally. *See* IOSCO, CONSULTATION REPORT ON POLICY RECOMMENDATIONS FOR CRYPTO AND DIGITAL ASSET MARKETS (May 2023), available at
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf.

Table of Contents

EXECUTIVE SUMMARY

DeFi commonly refers to financial products, services, arrangements, and activities that use distributed ledger or blockchain technologies (DLT), including self-executing code referred to as *smart contracts*. DeFi aims to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions, and by enabling certain direct investment activities.[3] DeFi is an important, evolving, and expanding technological innovation. The use of DLT may have the potential to foster financial innovation, increase efficiencies, and improve access to financial products, services, and activities. Proposed use cases for DLT include those relating to primary market issuance, secondary market trading, asset servicing and lifecycle management. While IOSCO encourages responsible innovation that benefits investors and the markets, it has prioritized the need to focus on analyzing and responding to market integrity and investor protection concerns, including those emerging from technological developments in DeFi.

This consultation report proposes nine policy recommendations that IOSCO plans to finalize by the end of 2023 to address market integrity and investor protection concerns arising from DeFi by supporting greater consistency of regulatory frameworks and oversight in member jurisdictions. They are complementary to the Policy Recommendations for Crypto and Digital Assets (CDA) Markets[4] issued for consultation in May 2023. The two sets of IOSCO recommendations have been developed in accordance with IOSCO's Crypto-Asset Roadmap (Roadmap) published in July 2022.[5]

The proposed recommendations follow a 'lifecycle' approach in addressing the key risks identified in this report. They are principles-based and outcomes-focused, and aimed at DeFi products, services, arrangements, and activities by applying IOSCO's widely accepted global standards for securities markets regulation.

[3] *DeFi* is a term used in industry and broader discussions. It does not give rise to a unique or different legal arrangement. Currently, there is no generally accepted definition of *DeFi,* even among industry participants, or what makes a product, service, arrangement, or activity decentralized. While DeFi may seek to eliminate traditional intermediaries, this report notes that certain DeFi arrangements and activities are in fact providing products and services that are equivalent to those provided by traditional market intermediaries and may be treated as market intermediaries in a particular jurisdiction.

[4] IOSCO, POLICY RECOMMENDATIONS FOR CRYPTO AND DIGITAL ASSET MARKETS CONSULTATION REPORT (May 2023), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf.

[5] *See* IOSCO, CRYPTO-ASSET ROADMAP FOR 2022-2023 (July 2022), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD705.pdf. The FTF was established in March 2022 to develop recommendations to the Board of IOSCO and thereafter to oversee the implementation of IOSCO's regulatory agenda for Fintech and crypto-assets. The FTF is prioritising policy-focused work on crypto-asset markets and activities in its initial 12 to 24 months of operation, while continuing to monitor market developments associated with broader Fintech-related trends and innovation.

One of IOSCO's goals is to promote greater consistency with respect to the regulation and oversight of crypto-asset activities, given the cross-border nature of the markets, potential for regulatory arbitrage and significant risk of harm to retail investors. IOSCO is also seeking to encourage consistency in the way crypto-asset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of "same activity, same risk, same regulatory outcome."

The proposed recommendations also cover the need for enhanced cooperation among regulators to coordinate and respond to cross-border challenges in enforcement and supervision, and to address regulatory arbitrage concerns, that arise from the cross-border nature of global crypto-asset activities conducted by DeFi participants who often offer their products and services across multiple jurisdictions.

While the proposed recommendations are not directly addressed to market participants, all participants in crypto-asset markets are strongly encouraged to carefully consider the expectations and outcomes articulated through the proposed recommendations and the respective supporting guidance in the conduct of regulated and cross-border activities.

SECTION I. INTRODUCTION TO THIS CONSULTATIVE REPORT

Background

In March 2022, IOSCO published its Decentralized Finance Report (2022 Report), presenting a comprehensive description of the DeFi market as of the date of that report.[6] Since the 2022 Report, the use of DLT-based applications has increased in scale and scope, with some predicting continued growth in this area in the coming years.[7] The 2022 Report noted that it is important for IOSCO members to develop a holistic and comprehensive understanding of the DeFi market, including by identifying and analyzing, among other things, the structural components of the DeFi market, the participants and activities involved, and the products and services offered.

Objectives of the Report

Consistent with the Roadmap, the present report is intended to build on the 2022 Report by providing recommendations and guidance to IOSCO members as they analyze DeFi within their own regulatory frameworks. While recognizing the value of responsible innovation, this report seeks to make clear that market regulators globally should apply a "same activity, same risk, same regulatory outcome" approach to financial markets, regardless of the technology that may be used to deliver financial products and services. In certain jurisdictions, this could mean that existing laws and regulations apply. To facilitate a level-playing field between crypto-asset markets and traditional financial markets and to reduce the risk of regulatory arbitrage, regulatory frameworks for DeFi (existing or new) should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those required in traditional financial markets.

Like the 2022 Report, this report emphasizes the need for regulators to understand the DeFi market and its significance, what financial products and services are offered, who is offering those products and services, and to whom regulatory obligations may apply. This report is intended to assist IOSCO members reach that understanding based on their own analyses. As the 2022 Report notes, applicable regulatory frameworks apply to DeFi products, services, arrangements, and activities, notwithstanding characterizations or assertions of decentralization by market participants.

[6] *See* IOSCO, DECENTRALIZED FINANCE REPORT (Mar. 2022), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf [hereinafter 2022 Report"]. The 2022 Report contains a detailed explanation of terms used in the 2022 Report and in this report. While each report cites to a number of sources, much of the reports' content represents a compilation of information developed by examining publicly available sources, including websites, white papers, and software code, including smart contract code. Not all of these sources have been cited.

[7] *See* BCC PUBLISHING, GLOBAL DECENTRALIZED FINANCE (DEFI) MARKET: TRENDS, GLOBAL SCENARIO, INNOVATIONS & MARKET (Jan. 2023), available at https://www.bccresearch.com/market-research/finance/global-decentralized-finance-market.html.

The report aims to assist global regulators as they identify the "**Why, What, Who, and How**" in applying IOSCO's Objectives and Principles for Securities Regulation and relevant supporting IOSCO standards, recommendations, and good practices (hereinafter IOSCO Standards) and their own regulatory frameworks to DeFi.

- ***Why:*** The report describes the state of the DeFi market and why it presents significant investor and market risks, arising through participants operating in non-compliance with, or outside of, existing investor and market protection regulatory frameworks. Further, since the publication of the 2022 Report, the DeFi market has been prone to increasing exploits and attacks, illicit uses, and other misconduct, resulting in investor and market harm. Moreover, the ability to apply regulatory oversight is challenging, due in part to significant data gaps and technological complexities.
- ***What:*** The report describes the common products and services offered in the DeFi markets, demonstrating that they do not materially differ from products and services offered in traditional financial markets, and that they present the same risks, along with additional risks due to the way they are offered.
- ***Who:*** The report identifies the types of persons and entities typically involved in the development and provision of products and services using DLT-based components and offers ways to analyze their involvement to determine potential regulatory touchpoints.
- ***How:*** The report provides recommendations and guidance to regulators as they examine the application of IOSCO Standards, and existing or new frameworks within their own respective jurisdictions, to DeFi products, services, arrangements, and activities.

Acknowledging the definitional and interpretive jurisdictional differences that currently exist, IOSCO has developed the proposed recommendations and guidance in this report by developing a functional, economic approach to the analysis, assessment, and mitigation of DeFi risks, rather than seeking to develop a one-size-fits-all prescriptive taxonomy.

Accordingly, IOSCO is taking an outcomes-focused, principles-based approach to risk identification, assessment, and mitigation. This approach has been informed by a mapping of IOSCO Standards to DeFi products, services, arrangements, and activities, and has enabled IOSCO to examine and assess how its existing policy framework aligns with key risks identified in DeFi.

Topics Covered in the Report

Section I (Introduction) introduces the report and describes its high-level objectives.

Section II (State of the DeFi Market) and the accompanying Annexes provide an overview of the state of DeFi, highlighting developments since the 2022 Report. These are intended to inform IOSCO members about the rapidly developing DeFi market through an analysis of recent events, trends and risks, and their implications for investors and the markets in DeFi.

Section III (High-Level Recommendations and Guidance) sets out nine policy recommendations that are intended to assist IOSCO members as they apply existing or develop new regulatory frameworks to achieve regulatory outcomes for investor protection and market integrity in DeFi that are the same as, or consistent with, those required in traditional financial markets.

The recommendations emphasize the importance of regulators developing a holistic and comprehensive understanding of DeFi products, services, arrangements, and activities.

This report recognizes that some jurisdictions have existing regulatory frameworks for financial instruments that encompass crypto and digital assets, including DeFi products, services, arrangements, and activities, while other jurisdictions are in the process of developing regulatory frameworks. Each jurisdiction should apply the IOSCO Standards, as they deem appropriate, within their existing or new frameworks.

Section IV (Questions for Public Consultation) contains consultation questions for public feedback.

Pre-Consultation Stakeholder Engagement

The proposed recommendations build on the analysis in the March 2022 report which benefited from broad consultation with IOSCO members, academics, and industry. These recommendations are informed by additional outreach with academics, data analytics firms, researchers, and technologists. The FTF also further surveyed its membership to identify key risks faced by regulators and policy measures needed to address the risks. Within its tight timelines, the FTF has also benefited from an initial discussion with its Affiliate Member Consultative Committee (AMCC) on the proposed framework now under consultation.

SECTION II. STATE OF THE DEFI MARKET

The 2022 Report provided a comprehensive overview of the DeFi market, including DeFi products, services, arrangements, and activities, based on information available at the time of its publication. This section (and the accompanying Annexes) provides: (A) an overview of DeFi's common products and services; (B) an update on recent developments and trends; (C) an overview of DeFi exploits, attacks, and illicit uses; (D) an explanation of data gaps and challenges; and (E) a highlight of key risks and considerations.

A. Common Products and Services Using DLT

Persons and entities are currently offering financial products and services that, at least in part, utilize code deployed on public permissionless DLT-based platforms. These products and services include the offering of financial instruments; trading, lending, and borrowing activities involving financial instruments; and the provision of services relating to financial instruments, including exchange, broker, dealer, asset management, custody, clearing, and settlement.

A common misperception is that DeFi products and services are materially different from those found in traditional financial markets. Another common misperception is that DeFi products and services are offered in a fully automated manner using smart contracts, with no human involvement. However, these are not accurate descriptions of how the DeFi market currently operates in practice. Most of the products and services referred to as DeFi mimic those of traditional financial markets. Moreover, the code that implements a DeFi protocol is created, deployed, operated, and maintained by humans; it does not just spontaneously materialize and self-execute. Further, the smart contracts operating on a blockchain typically are only one component of the product or service being offered. For the most part, the products and services referred to as DeFi are offered by persons or entities using traditional components and infrastructures as well as smart contracts and blockchains.[8]

The 2022 Report details various DeFi products and services commonly offered. The DLT-based components associated with these products and services are commonly referred to as DeFi protocols. Typical DeFi protocols include, for example, decentralized exchange protocols, lending/borrowing protocols, and aggregator protocols. The 2022 Report described the way that these protocols typically operate in detail in, and this report provides an abbreviated description below for ease of reference.

Decentralized Exchange (DEX)[9]

A DEX provider typically provides a service through which one type of crypto-asset can be traded for another. One type of DEX is known as an *order book* DEX where, typically, a central operator maintains a user interface (such as a website or mobile application) and an off-chain order book, with a blockchain primarily serving as a settlement layer. Users

[8] *See* 2022 Report, *supra* note 5, at 7-8.

[9] *Id.* at 14-15.

interested in buying or selling a particular crypto-asset at a certain price (makers) communicate their order to the operator, who will in turn publish the order for the use of other participants who may be interested in matching the order (takers). Once there is a match, the taker typically submits the order to the DEX, which sends the matched order for execution and settlement on a blockchain. Unlike in a centralized trading platform context, the operator may never have control of the users' crypto-assets and may serve only as a *relayer* of information that is necessary for the trade to be executed and settled on the blockchain. The operator typically collects fees from makers and takers for providing this service. In addition, takers typically pay a fee on each trade, a portion of which may go to makers to reward them for providing liquidity.

Another type of DEX uses what are referred to as "automated market makers" (AMMs). Operators of this type of service typically create a "factory" (or set) of smart contracts that can be used by participants to deposit two or more crypto-assets into what is commonly called an AMM or "liquidity pool", which then is available for other participants who want to exchange one of those crypto-assets for another. Depositors to the liquidity pool are generally referred to as "liquidity providers." They typically deposit a number of crypto-asset pairs into the liquidity pool and receive in return a crypto-asset, often referred to as a "liquidity provider token" or "LP token," which 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 between A and B is automatically determined according to a preset formula that is based on the ratio of assets held by the pool and is designed to programmatically adjust prices to match market prices. 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 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. AMM-based DEXs are substantially dependent on arbitrage traders, typically employing bots, who are programmed to buy or sell crypto-assets for profit until its liquidity pool price converges with the average market price.

Lending/Borrowing[10]

Providers of lending/borrowing protocols offer a service that allows holders of crypto-assets, often stablecoins,[11] to earn a fixed or variable return on those assets by depositing

[10] *Id.* at 11-12.

[11] The term "stablecoin" commonly refers to a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. *See, e.g.,* FSB, HIGH-LEVEL RECOMMENDATIONS FOR THE REGULATION, SUPERVISION AND OVERSIGHT OF GLOBAL STABLECOIN ARRANGEMENTS 19 (July 2023), available at https://www.fsb.org/wp-content/uploads/P170723-3.pdf. There is no universally agreed definition of stablecoin. The term stablecoin does not denote a distinct legal or regulatory classification. Importantly, the use of the term "stablecoin" in this report is not intended to affirm or imply that the asset's value is necessarily stable or that it is a type of currency. Rather, the term is used here because it is commonly employed by market participants

them in a smart contract (or lending pool) that simultaneously allows other participants to borrow those assets. Depositors typically receive a different crypto-asset, which represents that depositor's *pro rata* interest in the lending pool and can be redeemed at any time for the amount of the original deposit and accrued interest. In many such services, interest rates can vary and can be set by algorithms, a protocol project team, or through certain governance voting. Loans can be set 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. 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. Loans are generally required to be over-collateralized.

Aggregator[12]

Providers of *aggregator* services offer users a means to optimize trading, liquidity, or yield-generating opportunities, typically by scanning across protocols for such opportunities and then routing transactions to fulfill desired user parameters. Aggregators allow users, for example, to source trading bids and offers, monitor prices, and transact with a number of protocols from a single interface. Based on the activity being facilitated, aggregators typically include *DEX aggregators* (that query a range of trading protocols for the purpose of finding the best terms for a trade, including optimal trading price, trading fee and *slippage* (i.e., changes in deal terms over time)); *yield aggregators* (that collect user deposits and distribute deposits among protocols, using various strategies to maximize returns); and *portfolio aggregators* (that monitor a user's portfolio of crypto-assets across blockchains and protocols, and may facilitate the management of or trading in the portfolio). Certain aggregators may also function as an aggregator of aggregators, for example, by scanning various DEX aggregators to identify the best trade terms available. Aggregators may charge a fee for their services, which is added to the fee(s) that are otherwise charged by the protocols with which they interact.

DeFi: The Big Picture (Enterprise Level Viewpoint)

Importantly, as the 2022 Report points out, DeFi protocols (and the smart contracts that they use) typically are only one component of a larger enterprise that carries out the provision of any particular product or service. At the enterprise level viewpoint, persons and entities are engaging in real-world activities, facilitated through the use of various technologies (both on-chain and off-chain) to provide financial products and services. Those persons and entities at the enterprise level are described in the 2022 Report as the

and authorities. *See* FSB, REGULATION, SUPERVISION AND OVERSIGHT OF "GLOBAL STABLECOIN" ARRANGEMENTS (Oct. 2020), available at https://www.fsb.org/wp-content/uploads/P131020-3.pdf; *see also* BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 7 (July 2023), available at https://www.bis.org/publ/othp72.pdf (discussing a number of shortcomings that threaten stablecoins' claims to stability, including that the quality and transparency of reserve assets is often lacking).

[12] 2022 Report, *supra* note 5, at 15-16.

Big Picture. There are a number of primary participants involved at the enterprise level, including those engaging in capital formation, development, and deployment of the components necessary to provide a product or service (such as founders, developers, and foundations); those investing in and using the product or service (such as investors, traders, lenders, and borrowers); those contributing to the ongoing operations of the enterprise (including those with control or sufficient influence over the governance of the enterprise); and those providing infrastructure and services around the product or service (such as oracles, bridges, and miners/validators). Each of the stakeholders in any particular arrangement plays an important role and generally expects to earn a profit through participation. As regulators determine appropriate regulatory touchpoints, they will likely find it useful to examine any particular DeFi arrangement and activity at the enterprise level.

In analyzing DeFi arrangements and activities at the enterprise level, it is important to note that, although persons and entities may be using technologies to conduct their business operations in ways that may differ in certain respects from traditional providers, the products and services they provide do not materially differ from those in traditional markets.[13] Upon close examination, these stakeholders and their roles, and the organizational, technological, and communication mechanisms they use, tend to mimic those that regulators are used to seeing in traditional finance. Therefore, the choices of persons, for example, to organize as a Decentralized Autonomous Organization (DAO) (instead of incorporating); to communicate using internet-based communications platforms (instead of meeting in a physical location or boardroom); to issue crypto-assets (instead of engaging in more traditional forms of fund raising); and to deploy code using computers organized in a peer-to-peer network structure (instead of using a server-client network structure), do not abdicate these persons and entities of their regulatory responsibilities. Regardless of the labels, organizational forms, or technologies used, persons and entities who provide financial products and services are subject to applicable laws.

The *Big Picture* diagram in **ANNEX D** (reproduced from the 2022 Report) illustrates a common scenario describing participants and activities sin DeFi. It can serve as a useful guide for regulators as they analyze any particular DeFi product or service at the enterprise level.

B. Growth of DeFi and the Impact of Recent Market Developments on DeFi Investors and Markets

[13] *See* FSB, THE FINANCIAL STABILITY RISKS OF DECENTRALISED FINANCE 1 (Feb. 2023) available at https://www.fsb.org/wp-content/uploads/P160223.pdf [hereinafter "FSB DeFi Report"] ("While the processes to provide services are in many cases novel, DeFi does not differ substantially from TradFi in the functions it performs.").

Fuelled by the use of stablecoins and an influx of participants through centralized crypto-asset platform on-ramps, the combined Total Value Locked (TVL)[14] of the DeFi ecosystem rose dramatically in 2021 and reached a reported all-time high of approximately $180 billion in November 2021. However, the occurrence of several significant crypto-asset market events since the publication of the 2022 Report have had an impact on the DeFi ecosystem, which has led to investor losses and market disruptions. These events have revealed vulnerabilities in the broader crypto-asset market and have demonstrated the close but often hidden interconnectedness and interdependencies between and among crypto-asset market participants across the crypto-asset ecosystem, including DeFi arrangements and activities. These events demonstrate that shocks to one part of the crypto-asset market, including from events occurring on centralized crypto-asset platforms and involving stablecoins, as well as shocks to traditional financial markets, likely will have spill-over effects into DeFi, impacting investors and the markets.[15]

For example, in 2022, the algorithmic stablecoin[16] Terra USD and its associated LUNA token death spiraled, reportedly resulting in billions of dollars in outflows from DeFi applications associated with Terra, as well as the halting of the Terra blockchain.[17] Also in 2022, the insolvency of FTX, at the time one of the largest centralized crypto-asset platforms globally, reportedly impacted certain DeFi protocols and ecosystems with which FTX was associated or had supported, and also impacted FTX's customers, counterparties and investors, with propagating effects into DeFi protocols with whom those parties had interlinkages.[18] In 2023, a New York State supervisory action ordering Paxos Trust Company to cease minting the stablecoin BUSD reportedly caused certain centralized platforms and DeFi protocols to limit the use of BUSD, with some DeFi protocols taking

[14] Total Value Locked (TVL) is an industry reported measure calculated by multiplying the token market value by the number of tokens deposited into a particular DeFi protocol, blockchain, or ecosystem. While TVL has become a metric for gauging interest in a particular crypto-asset sector and can be looked to in a relative sense, it will change with the market value of the tokens it counts and may "double-count" tokens.

[15] *See* FSB DeFi Report, *supra* note 12, at 18.

[16] An "algorithmic stablecoin" is a stablecoin that purports to maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoin in response to changes in demand. *See* FSB, HIGH-LEVEL RECOMMENDATIONS FOR THE REGULATION, SUPERVISION AND OVERSIGHT OF GLOBAL STABLECOIN ARRANGEMENTS 17 (July 2023), available at https://www.fsb.org/wp-content/uploads/P170723-3.pdf.

[17] *See, e.g.,* Krisztian Sandor & Ekin Genç, *The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA*, COINDESK (Dec. 22, 2022, 4:07 pm), https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/.

[18] FTX operated (and other centralized crypto-asset platforms operate) as a multifunctional crypto-asset intermediary, which typically provides a vertically integrated suite of products and services within one entity or group of affiliated entities. This operational structure poses significant risks. *See* CDA Report (describing in detail the significant risks presented by such operational structure). The interconnectedness and interdependencies of centralized crypto-asset platforms with DeFi arrangements and activities, detailed herein and in the 2022 Report, exacerbate risks in DeFi.

steps to freeze their BUSD markets.[19] Also in 2023, the failure of a US regional bank that offered deposit services to a stablecoin issuer contributed to a temporary de-pegging of the stablecoin because of uncertainty about the issuer's access to its deposits.[20] This, in turn, caused disruptions in the DeFi markets. These recent events and their respective impacts in DeFi are explained in greater detail in **ANNEX A** to this report.

Each of these consequential events had a noticeable impact, not only on particular DeFi arrangements and activities at the time of their occurrence (or shortly thereafter), but on the entire DeFi ecosystem as well. In the first week of May 2022, before the collapse of Terra USD/LUNA, the reported combined TVL of the DeFi ecosystem was approximately $140 billion. By May 14, 2022, that number fell to approximately $80 billion. In the wake of FTX's collapse, the reported combined TVL fell further to approximately $40 billion. Reported combined TVL has thus far somewhat stabilized in 2023, fluctuating with the volatility of its underlying crypto-assets, but has remained at approximately only a third of the level it was in April 2022 before Terra USD/LUNA's collapse.[21]

C. DeFi Exploits, Attacks and Illicit Uses

The 2022 Report discussed vulnerabilities associated with products and services that rely on DLT-based arrangements and activities. This report explores in greater depth in **ANNEX B** how cyber exploits and attacks continue to target these vulnerabilities and have resulted in massive losses for investors and other DeFi participants. Vulnerabilities can exist, for example, in blockchain networks, smart contracts and protocols, governance mechanisms, oracles, and cross-chain bridges. At a high level, exploits and attacks in DeFi target access control points. When such points are compromised, an attacker can, for example, commandeer the ability to alter token balances, interfere with governance processes, change the initial parameters and functionality of a smart contract, and circumvent protections such as multi-signature (multi-sig) procedures.

According to one blockchain analytics firm, attacks on DeFi protocols in 2022 accounted for 82.1% of all crypto-assets stolen by hackers — a total of $3.1 billion — up from 73.3% in

[19] *See New York regulator says Paxos unable to "safely" issue Binance's stablecoin*, REUTERS (Feb. 13, 2023, 10:01 am), https://www.reuters.com/article/fintech-crypto-binance-stablecoin/new-york-regulator-says-paxos-unable-to-safely-issue-binances-stablecoin-idUSL8N34T42O.

[20] *See* FSB, GLOBAL REGULATORY FRAMEWORK FOR CRYPTO-ASSET ACTIVITIES UMBRELLA PUBLIC NOTE TO ACCOMPANY FINAL FRAMEWORK 5 (July 2023), available at: https://www.fsb.org/2023/07/fsb-global-regulatory-framework-for-crypto-asset-activities/; *see also* BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 15 (July 2023), available at https://www.bis.org/publ/othp72.pdf ('The fall in crypto prices that started in the second half of 2022 did eventually spill over to the traditional financial system. … These cases highlight that a business model that is highly exposed to crypto can be problematic for the banking sector.').

[21] *See* DEFILLAMA, https://defillama.com/. The total market value of crypto-assets reportedly reached nearly $3 trillion in mid-November 2021, but has declined to approximately one-third that value currently. *See, e.g.,* CoinGecko, Cryptocurrencies Global Charts, available at https://www.coingecko.com/en/global-charts.

2021. Of that $3.1 billion, 64% was attributable to attacks on cross-chain bridges.[22] Another blockchain analytics firm reported that nine of the ten largest attacks occurred against DeFi projects.[23] Reports indicate that hacker groups associated with North Korea are among the most prolific.[24] Reportedly, North Korean-linked hackers have stolen $1.1 billion in crypto-assets through hacks of DeFi protocols.[25]

Recent reports also assert that DeFi protocols increasingly are used for money laundering and other illicit uses.[26] Reports describe the use of DeFi protocols as a means to convert stolen crypto-assets of one type for crypto-assets of another type that is more liquid or less volatile and, eventually, these crypto-assets can be converted into fiat currencies at centralized crypto-asset trading platforms. One blockchain analytics firm estimates that hackers holding stolen crypto-assets send a majority of those funds (57%) to DeFi protocols.[27] A recent report by the Financial Action Task Force (FATF) found that crypto-assets pose money laundering, terrorist financing, and proliferation financing risks, including abuse by sanctioned actors.[28]

D. Data Gaps and Challenges

Despite the existence of publicly available blockchain data and blockchain data analytics providers, regulators (and investors) face significant data gaps and challenges in understanding DeFi. Proponents of DeFi often claim that blockchain ecosystems are

[22] CHAINALYSIS, THE 2023 CRYPTO CRIME REPORT (Feb. 2023), available at https://go.chainalysis.com/2023-crypto-crime-report.html.

[23] TRM, ILLICIT CRYPTO ECOSYSTEM REPORT: A COMPREHENSIVE GUIDE TO ILLICIT FINANCE RISKS IN CRYPTO 32 (June 2023), available at https://www.trmlabs.com/illicit-crypto-ecosystem-report-2023#:~:text=TRM%20Labs%20data%20indicates%20that%20cryptocurrency%20wallets%20that%20receive%20victim,large%20transnational%20organized%20crime%20groups.

[24] *See, e.g.,* FATF, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 3 (June 2023), available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html ("Recent reports raise serious concerns about the threat posed by the Democratic People Republic of Korea's (DPRK) illicit VA-related activities, including ransomware attacks and sanctions evasion, for financing the proliferation of weapons of mass destruction. This activity has enabled an unprecedented number of recent launches of ballistic missiles (including inter-continental ballistic missiles). This threat is significant given both the scale of the funding (USD 1.2 billion worth of stolen VAs since 2017, including VAs stolen from DeFi arrangements) and the serious consequences of proliferation financing.") (internal citations omitted).

[25] CHAINALYSIS, *supra* note 21, at 60.

[26] *See id.*; U.S. DEPT OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE (Apr. 2023), available at https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[27] CHAINALYSIS, *supra* note 21.

[28] FATF, *supra* note 23, at 4 ("[DeFi] … pose[s] money laundering, terrorist financing and proliferation financing risks, including abuse by sanctioned actors. … Both jurisdictions and the private sector should strengthen efforts to monitor these risks, share approaches, and identify challenges to mitigate such risks, in addition to implementing the FATF Standards.").

completely transparent, given that smart contract code purportedly is publicly accessible and that activity on a blockchain is publicly observable. However, certain aspects of the DeFi ecosystem remain opaque and the data that is publicly accessible is difficult to access and interpret.

There exist several challenges to the accessibility and interpretability of relevant data, including:[29]

- ***Required skills and infrastructure:*** Accessing, cleaning, and standardizing data for analysis, including operational data sets from DeFi protocols and market data sets from the DeFi market more broadly, requires sophisticated software engineering and data science skills, as well as infrastructure. Interpreting and extracting insights from DeFi data sets also requires specific skills and infrastructure, including both financial market-related skills for traditional financial analysis, as well as computer science-related skills to interpret code and develop the necessary data pipeline and analytical infrastructure. Various datasets and analytical tools are also needed. In addition, while industry proponents claim that smart contracts are transparent, in practice the source code for smart contracts implemented on blockchains are in machine-readable (not human-readable) format, may not conform to public descriptions of the code (either in plain text or in a GitHub or GitLab repository of code), and in some cases may be subject to change by the smart contracts' developers.[30] As a consequence, what is *written* to a blockchain may need to be analyzed to determine whether it actually reflects what it is purported to represent.[31] Enhancements to the skills, datasets, and tools necessary to analyze DeFi data could improve a regulator's ability to oversee DeFi arrangements and activities.

- ***Lack of standardization:*** The lack of standardization across DeFi datasets and codebases makes it difficult to collect, reconcile, and analyze data across protocols, blockchains and markets.[32] Data providers may have materially different methodologies for aggregating data and calculating metrics. In addition to the lack of standardization in data sets, there is a lack of standardization in code used to develop DeFi protocols. For example, while there are open-source standards that describe the basic functionality for certain aspects of a token (e.g., ERC-20 standard) or DeFi service

[29] The Financial Stability Board has also discussed data challenges in a recent report. *See* FSB, *supra* note 12.

[30] Certain publicly available tools can be used, for example, to compile purported source code from GitHub for comparison to a smart contract's on-chain bytecode; however, use of such tools requires expertise and could require some standardization of data prior to using such a tool.

[31] For example, the US Securities and Exchange Commission recently filed a case alleging that, among other things, the promotors of a particular DeFi project merely uploaded transaction details to a blockchain, falsely claiming that the transactions had been processed and settled on the blockchain, when in reality they reflected payments made through traditional means off-chain. *See* https://www.sec.gov/litigation/complaints/2023/comp-pr2023-32.pdf.

[32] An example of operational data includes the number of addresses interacting with the protocol. An example of market data includes the volume of token swaps within a liquidity pool.

(e.g., liquidity pair smart contract), developers frequently modify code to provide additional functionality for their DeFi protocol. These modifications require analysts to examine each protocol individually to understand and extract relevant information. Compounding this complexity is the *composability* of smart contracts, which allows integrations between DeFi protocols or other smart contracts to create new systems or outputs. Composability can result in risks due to the various methods of integration and the reuse of existing software components. Further moves toward standardization across DeFi data sets and codebases could assist regulators in understanding and assessing DeFi arrangements and activities.

- ***Pseudonymity and Off-chain Activity:*** Another challenge to data analytics is the pseudonymous nature of transactional data on-chain and the opacity of data off-chain. Opacity can be exacerbated by the practice of market participants using multiple pseudonymous addresses to obfuscate their activity. This can lead to challenges in assessing, for example, levels of retail investor participation, concentrations in the market, interconnectedness within DeFi or to the broader financial ecosystem, or risks posed by a given market participant or activity. Improvements to recordkeeping and reporting could alleviate challenges to data analytics.

Such data gaps and challenges are pervasive in the DeFi ecosystem and are explored in greater detail in **ANNEX C**.

E. Key Risks and Considerations

As the 2022 Report noted, 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 is developing. In some jurisdictions, participants in the DeFi market may be operating in non-compliance with applicable laws and regulations. In others, participants may be operating outside the scope of existing regulatory frameworks. The 2022 Report identified key investor and market protection risks known in DeFi at that time and gave a detailed description of many of those risks, including risks arising from: asymmetry and fraud, market integrity issues, front-running (or similar activities), flash loans, market dependencies, use of leverage, illicit activity, operational and technology-based issues, cybersecurity issues, nascent stage of development, governance mechanisms, and the spill-over of risks to centralized/traditional markets. The risks identified in the 2022 Report continue to exist in DeFi today.

Events and trends observed since the 2022 Report have highlighted risks attendant to DeFi and the crypto-asset markets more broadly, including from market interconnectedness and interdependencies, the use of leverage, unpredictable and opaque governance structures, as well as risks from the structures of DLT-based arrangements themselves. The Financial Stability Board (FSB) recently released a report detailing the financial stability risks of DeFi (hereinafter FSB DeFi Report).[33] The FSB DeFi Report describes a panoply of risks, such as operational fragilities, liquidity and maturity mismatches, leverage, and

[33] FSB DeFi Report, *supra* note 12.

interconnectedness, and notes that these risks can be amplified by DeFi's technological features, the high degree of structural interlinkages among participants in DeFi, and from non-compliance with existing regulatory requirements or lack of regulation.[34] The FSB DeFi Report notes that, given the nascent and evolving nature of DeFi, severe market integrity issues could lead to potential impacts on financial stability, if the sector grows further and becomes more interconnected with traditional finance and the real economy.[35] The FSB DeFi Report specifically cites to the reliance of some DeFi products on continuous investor inflows to remunerate early adopters, a business model recognized as unsustainable.[36] A recent Bank for International Settlements (BIS) report concerning key risks of the crypto ecosystem, including DeFi, found that crypto has inherent structural flaws that pose serious risks not only to its own stability and safety, but also to that of the traditional financial system.[37]

The risk discussion in **ANNEX E** details some of the investor protection and market integrity risks in the DeFi market, particularly those associated with DeFi governance structures, derivatives and levered strategies, and the use of oracles and cross-chain bridges. More specifically, DeFi governance structures are often opaque, experimental, unpredictable, and/or easy to manipulate. Participation in such structures generally entails engagement with others on a pseudonymous or anonymous basis. This results in a lack of transparency into how governance mechanisms actually operate in practice, obfuscating the identity of controlling persons and masking conflicts and potential collusive behavior. The DeFi market also continues to offer exposure to levered strategies, exposing investors to well-known risks and also those exacerbated by features such as the automated liquidation of positions through smart contracts and hidden interlinkages. Furthermore, DeFi's reliance on connectivity to off-chain data and interoperability through oracles and cross-chain bridges continues to present considerable risks.

[34] *Id.* at 16.

[35] *Id.* at 23.

[36] *Id.*

[37] BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 1 (July 2023), available at https://www.bis.org/publ/othp72.pdf ("[W]hile DeFi mostly replicates services offered by the traditional financial system, it does not finance any activity in the real economy but amplifies known risks. As growth is driven mainly by the speculative influx of new users hoping for high returns, crypto and DeFi pose substantial risks to (especially retail) investors.").

SECTION III. RECOMMENDATIONS AND GUIDANCE

The following recommendations have been developed based on information and analysis from the 2022 Report; subsequent events, developments, and analysis; a survey to IOSCO members (the results of which are described in **ANNEX G**); and public source research and outreach to industry, academic and researchers. The recommendations and guidance describe how regulators can analyze DeFi products, services, arrangements, and activities, and are intended to support those authorities in jurisdictions seeking to apply IOSCO's Standards to DeFi through existing regulatory frameworks, as well as those authorities that are considering new frameworks to address any potential gaps in order to achieve regulatory outcomes that are the same as, or consistent with those that are required in traditional financial markets.

In developing the guidance to the recommendations, a mapping was done of common DeFi products, services, arrangements, and activities across the IOSCO Principles for Securities Regulation, which includes a mapping of certain DeFi products, services, arrangements, and activities to those found in traditional finance. The complete mapping is found in **ANNEX F**. Portions of the mapping have been incorporated into the guidance to illustrate how regulators can apply IOSCO Principles through their own regulatory frameworks.

OVERARCHING RECOMMENDATION ADDRESSED TO ALL REGULATORS

Preamble: Intent of the Recommendations

The exposure of investors across the globe to DeFi has grown in recent years, as have investor losses amid regulatory non-compliance, financial crime, fraud, market manipulation, money laundering, and other illegal crypto-asset market activity. Given the similar economic functions and activities of the DeFi market and traditional financial markets, many existing international policies, standards and jurisdictional regulatory frameworks are applicable to DeFi products, services, arrangements, and activities.

IOSCO is issuing these proposed Policy Recommendations to help IOSCO members apply relevant existing IOSCO Standards through their own regulatory frameworks, as appropriate, to DeFi products, services, arrangements, and activities within their jurisdictions. These Recommendations recognize that some jurisdictions have existing regulatory frameworks that encompass DeFi, while other jurisdictions are in the process of developing regulatory frameworks. In addition, in some jurisdictions, the regulatory framework may allocate responsibility for the regulation and oversight of DeFi to a number of regulators that possess discrete and complementary mandates and objectives, to address investor protection and market integrity risks. Each jurisdiction should implement the Recommendations, as they deem appropriate, within their frameworks considering each regulator's role within those existing or developing frameworks, and the outcomes achieved through the operation of the frameworks in each jurisdiction.[38]

These Recommendations should be considered by IOSCO members as they apply existing regulatory frameworks (*Existing Frameworks*), or as they are granted new powers and/or are developing new requirements (together *New Frameworks*), to DeFi and related activities in a manner that achieves outcomes across jurisdictions consistent with IOSCO Standards, including the IOSCO Objectives and Principles for Securities Regulation.

These Recommendations and guidance form part of IOSCO's efforts within the broader context of cooperation and coordination with respect to DeFi among international bodies such as the FSB, FATF and the BIS, and between the Standard Setting Bodies such as IOSCO, the Committee on Payments and Market Infrastructures-IOSCO (CPMI-IOSCO) and the Basel Committee on Banking Supervision (BCBS). This should help facilitate a level playing field between crypto-asset markets and traditional financial markets and help reduce the risk of regulatory arbitrage arising from any differences in how the rules are applied and enforced with respect to DeFi and traditional financial markets.

As discussed herein, DeFi products and arrangements may fall within the definitions of securities or other regulated financial instruments in a jurisdiction's Existing Framework or New Framework. However, in jurisdictions where such products and arrangements do not, regulators are encouraged to analyze the applicability and adequacy of their regulatory frameworks, and the extent to which (1) such products and arrangements behave like substitutes for securities or other regulated financial instruments, and (2) investors have substituted securities or other financial instrument investment activities with DeFi investment activities.[39]

INTEROPERABILITY WITH IOSCO POLICY RECOMMENDATIONS FOR CRYPTO AND DIGITAL ASSET MARKETS

In May 2023, pursuant to its Roadmap, IOSCO published its Policy Recommendations for Crypto and Digital Asset Markets Consultation Report (CDA Report), containing recommendations aimed at the activities performed by crypto-asset service providers (CASPs).[40] CASPs are service providers that conduct a wide range of activities relating to

[38] Given the diversity of operating landscapes across different jurisdictions, the application and/or implementation of the Recommendations can take into account the context of specific legal structures prevailing in each jurisdiction, as well as the respective mandates of individual regulators where relevant. One way for a regulator to accomplish this, through its given mandate and the regulatory frameworks it applies, is to set out clear principles-based expectations for a DeFi participant to meet (which can be supported by regulatory guidance, as appropriate), in order to achieve the same regulatory outcomes articulated in this report.

[39] For such jurisdictions, this report may be read and interpreted to mean that the recommendations apply as though the DeFi products and arrangements are within the definition of securities or other regulated financial instruments, and jurisdictions should look to achieve the outcomes set out in the recommendations, as appropriate and consistent with their respective mandates.

[40] *See* CDA Report, *supra* note 17, at 1.

crypto-assets,[41] including but not limited to, admission to trading, trading (as agent or principal), operating a market, custody, and other ancillary activities such as services relating to lending/staking of crypto-assets and the promotion and distribution of crypto-assets on behalf of others. These service providers can exist as centralized crypto-asset service providers, which operate under traditional corporate forms, and they can also exist in DeFi, where said activities can be carried outside of traditional corporate forms.

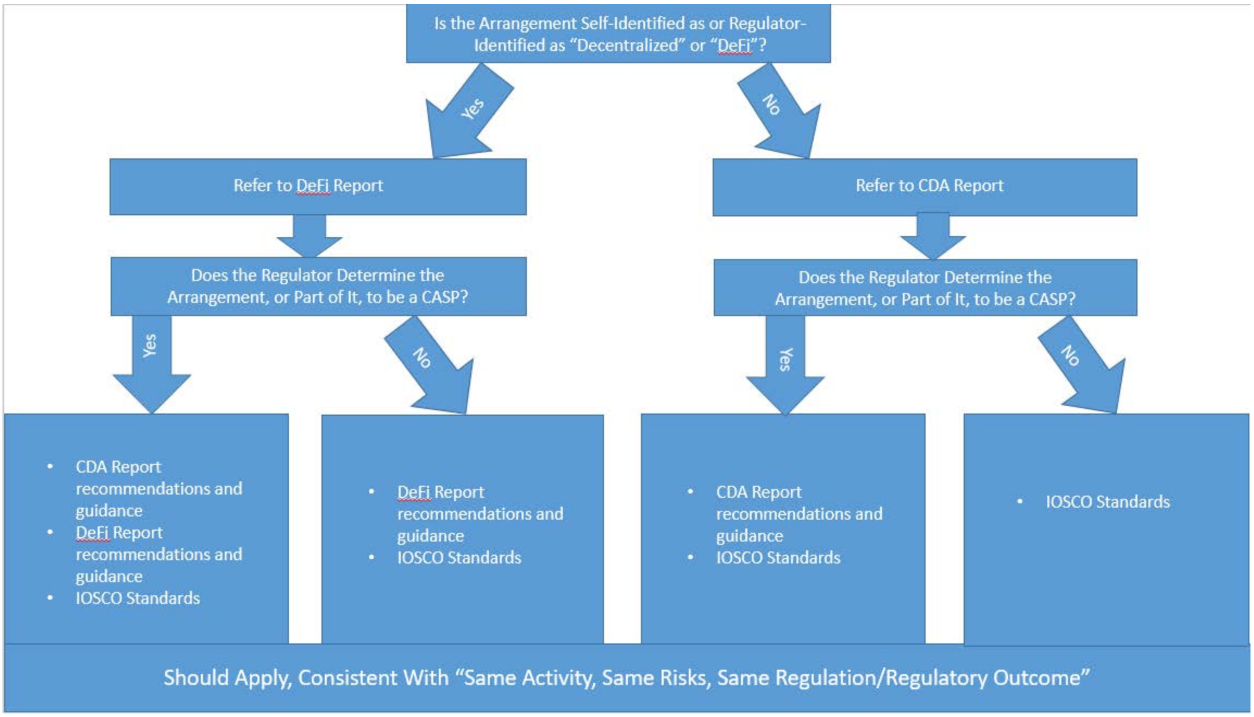
The delineation between centralized and decentralized finance (or CeFi and DeFi) is more a spectrum than a bright line. In the crypto-asset markets, along a spectrum of arrangements, persons and entities typically engage in financial activities that substantially mirror traditional financial activities. They do so using a number of technologies including, to varying degrees, DLT. However, regardless of the organizational form or technologies used, these persons and entities should be treated in line with the guiding principle of "same activity, same risk, same regulatory outcome."

IOSCO recognizes that regulatory touchpoints are readily identifiable where persons and entities are organized in traditional corporate forms. However, as noted, persons and entities who provide DeFi products and services attempt to arrange and distribute their operations outside of traditional corporate forms. Thus, it is possible that, in certain instances, it may be more challenging to identify regulatory touchpoints to which regulatory obligations may be applied. This report is thus intended to foster a deeper understanding of the DeFi market as currently operating to assist regulators with their analysis.

The recommendations and guidance in this report should be applied to a particular arrangement if it identifies itself or is identified by a regulator as decentralized. This report provides a diagnostic (i.e., understanding the facts and circumstances of an activity) and prognostic (i.e., understanding the investor risks and market risks posed by the activity) approach to examining and assessing DeFi arrangements, such that for a particular activity and its risks, regulators can apply the same regulation or aim to achieve the same regulatory outcome.

To the extent a regulator, applying the recommendations in this report, determines that a particular DeFi arrangement, or a part of that arrangement, falls within the scope of the definition of a CASP, the CDA Report recommendations will also apply to the CASP and the provision of related regulated activities. Thus, whatever form or organization the CASP takes, if a person or entity is a CASP in a particular jurisdiction, the recommendations of the CDA Report will also apply to the CASP. The flow chart below illustrates the interoperability of the CDA Report and this DeFi report:

[41] The term "crypto-asset," also sometimes called a "digital asset," refers to an asset that is issued and/or transferred using DLT, including, but not limited to, so-called "virtual currencies," "coins," and "tokens." To the extent digital assets rely on cryptographic protocols, these types of assets are commonly referred to as "crypto-assets."


Is the Arrangement Self-Identified as or Regulator-Identified as "Decentralized" or "DeFi"?
Yes
No
Refer to DeFi Report
Refer to CDA Report
Does the Regulator Determine the Arrangement, or Part of It, to be a CASP?
Yes
No
Does the Regulator Determine the Arrangement, or Part of It, to be a CASP?
Yes
No
CDA Report recommendations and guidance
DeFi Report recommendations and guidance
IOSCO Standards
DeFi Report recommendations and guidance
IOSCO Standards
CDA Report recommendations and guidance
IOSCO Standards
IOSCO Standards
Should Apply, Consistent With "Same Activity, Same Risks, Same Regulation/Regulatory Outcome"

Markets participants are strongly encouraged to carefully consider the expectations and outcomes articulated through the proposed recommendations and the respective supporting guidance, including, for CASPs, the recommendations and guidance in the CDA Report.

Recommendation 1 – Analyze DeFi Products, Services, Arrangements, and Activities to Assess Regulatory Responses

A regulator should analyze DeFi products, services, arrangements, and activities occurring or located within its jurisdiction with a view to applying its Existing Framework or New Framework, as appropriate, in accordance with the principle of "same activity, same risk, same regulatory outcome." To do so, a regulator should aim to achieve a holistic and comprehensive understanding of such DeFi products, services, arrangements, and activities. A regulator should assess what technological knowledge, data, and tools the regulator needs to understand, and analyze DeFi products, services, arrangements, and activities to inform regulatory responses.

Guidance

Understanding DeFi products, services, arrangements, and activities occurring or located within a jurisdiction is critical to determining the appropriate regulatory response, including, the potential application of IOSCO Standards through applicable regulatory frameworks.

The 2022 Report recognized that a comprehensive understanding of the regulatory implications arising from DeFi requires analyzing the totality of the DeFi ecosystem as it exists currently, its interrelationship with centralized crypto-asset platforms and service providers and traditional markets and activities as well as anticipating how it may continue to develop in the future. Developing a comprehensive understanding involves identifying and analyzing, among other things, the structural components of DeFi products, services, arrangements, and activities; the roles of each of the participants involved, including their incentives and motivations; how participants engage with the various components and each other; and the roles that centralized crypto-asset platforms and service providers play.

In assessing whether a particular product, service, arrangement or activity falls within a regulator's jurisdictional remit, ideally the regulator should aim to gain a holistic understanding of the particular product, service, arrangement and activity at (i) an enterprise level (i.e., based on the factual and substantive economic reality), (ii) a functional level, and (iii) a technical level.

The regulator should seek to understand the DeFi arrangement at the economic reality level, or the "enterprise level." In so doing, the regulator should seek to understand how each of the participants involved in the particular DeFi arrangement are involved at all stages in the life-cycle of the arrangement. For example, the regulator should seek to ascertain how the particular arrangement was developed and founded, promoted and funded, and how it is operated, used and maintained. The regulator should seek to ascertain how income, revenues and profits are generated, including any fee structures. This includes understanding the life-cycle of any associated tokens. The regulator should also seek to understand the interrelationship of each of the participants with each other, including centralized crypto-asset platforms and traditional markets and activities. The *Big Picture* diagram (depicted in **ANNEX D**) and the 2022 Report identify and describe various participants, and their activities, fund flows, and interrelationships. The *Big Picture* diagram and 2022 Report can serve as guides to a regulator seeking an economic reality or enterprise level view of any particular arrangement in DeFi. Critically, the regulator should seek to ascertain how decisions are made at the enterprise level. In many cases, identifying who exercises control or sufficient influence at the enterprise level will reveal existing or potential regulatory touchpoints.

When examining any particular DeFi arrangement, a regulator could consider a review of publicly available information concerning the DeFi arrangement, including from sources such as websites, white papers, industry reports, and social media. They could also consider engaging with persons involved with or associated with the arrangement, as well as experts, academics, researchers and public advocacy groups, as appropriate. Further, they could consider using available investigatory tools and techniques to gather additional information, including relevant information sharing arrangements with other authorities located within and outside their jurisdiction.

A regulator should also seek to analyze the DeFi arrangement at the functional level. A regulator should seek to understand the activities being conducted by or through the DeFi arrangement and, in particular, what products and/or services are being provided. Many of the financial products and services in DeFi mirror, and in some cases overlap with, more traditional securities and other regulated financial instruments and related products and services. A potential starting point for this analysis is to map the particular DeFi arrangement to traditional financial products and services. The 2022 Report, which includes comparisons between DeFi activities and traditional financial activities, can serve as a starting point for analysing the common types of DeFi arrangements. The mapping in the guidance under Recommendation 3 below can provide further assistance.

A regulator also could seek to analyze the DeFi arrangement at the technical level, if feasible. Although analysis at the technical level requires the necessary knowledge, data and tools, such analysis is helpful to fully understand and analyze DeFi products, services, arrangements, and activities. This type of analysis requires understanding the relevant technologies in the *tech stack* associated with the DeFi arrangement.[42] For example, regulators may seek to understand how the *settlement layer* blockchain operates, including what type of consensus mechanism the settlement layer uses, the concentration of participants in the consensus mechanism, and to what degree they may impact the functioning of a smart contract or protocol, including through the inclusion or ordering of transactions (in connection with *maximal extractable value* (MEV) strategies) or by exerting some other control over the DeFi arrangement. The analysis may also include an understanding of how the arrangement's associated smart contracts work, what other technologies and processes the arrangement relies upon (on-chain and off-chain, including bridges and oracles), and what role particular crypto-assets play in the operation of the arrangement. It may also require an understanding of how, technologically, a user interacts with the arrangement, i.e., through various user interfaces, and how those interfaces are controlled and maintained.

Regulators may need to consider whether they have the appropriate resources to evaluate DeFi products, services, arrangements, and activities. Regulators should assess whether there are limitations on their ability to identify appropriate participants that may be subject to regulation. If there are any such limitations, regulators should assess the cause for the limitation – whether regulatory, legal, resource/knowledge-based, or otherwise – and whether and how those can be addressed. If a regulator lacks the capacity to undertake a technical level analysis, the regulator could consider how it might augment its capacity or seek technical assistance.

Further, regulators should seek methods to obtain verifiable data and information about DeFi products, services, arrangements, and activities as they engage in such analysis. This may include the use of blockchain analytical tools and techniques for on-chain data and the use of supervisory, examination and investigatory tools and techniques for on-chain and off-chain data. When considering crypto-asset related data, it is important to bear in mind that on-chain data can be difficult to decipher without the required tools and expertise and is often pseudonymous or anonymous. Off-chain data, such as that available from crypto-asset trading platforms, typically is not audited or otherwise verified. **ANNEX C** provides a detailed analysis of data gaps and challenges in DeFi.

[42] *See* 2022 Report, *supra* note 5, at 3-4.

Regulators could consider how best to communicate and engage with DeFi market participants and others (such as academics, researchers, and public policy groups) as they evaluate DeFi products, services, arrangements, and activities within their jurisdictions and apply existing or new frameworks.

Recommendation 2 – Identify Responsible Persons

A regulator should aim to identify the natural persons and entities of a purported DeFi arrangement or activity that could be subject to its applicable regulatory framework (Responsible Person(s)).[43] These Responsible Person(s) include those exercising control or sufficient influence over a DeFi arrangement or activity.

Guidance

Responsible Person(s) generally are persons and entities that provide or actively facilitate the provision of products or services. Responsible Person(s) include those that maintain control or sufficient influence over a particular DeFi arrangement or activity.[44] Regulators can consider, for example, those with design and maintenance control; financial and economic control; and formal and legal control, among other things. In many cases, those who have control or sufficient influence over a particular activity at the enterprise level (see Recommendation 1 above) will also be Responsible Persons.

In conducting this analysis, a regulator should carefully examine any claim that the arrangement or activity is purportedly *decentralized* to the point that no persons or entities are responsible and should subject Responsible Persons to its applicable regulatory

[43] Responsible person(s) is meant broadly, to encompass, for example, natural persons, groups of persons, entities and organizations, whether formally or informally constituted.

[44] *See also* FATF, UPDATED GUIDANCE FOR A RISK-BASED APPROACH, VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 27 (2021), available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html ("[C]reators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a [Virtual Asset Service Provider ('VASP')] where they are providing or actively facilitating VASP services. This is the case, even if other parties play a role in the service or portions of the process are automated. Owners/operators can often be distinguished by their relationship to the activities being undertaken. For example, there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols. Countries may wish to consider other factors as well, such as whether any party profits from the service or has the ability to set or change parameters to identify the owner/operator of a DeFi arrangement. These are not the only characteristics that may make the owner/operator a VASP, but they are illustrative. Depending on its operation, there may also be additional VASPs that interact with a DeFi arrangement."). Indicia of control or influence can include, for example, ownership interest; significant financial interest; significant voting rights; management of or the ability to impact the operations of the protocol at an enterprise or fundamental level; the ability to set permissions or access rights for users of the protocol, or to otherwise impact the rights of other users of the protocol; control over user assets; and the ability to enter into agreements for the protocol or enterprise. What constitutes control may also depend on the relevant regulations in a jurisdiction.

framework. In assessing who is a Responsible Person, rather than relying on labels or concepts such as *decentralization* or the automated nature of smart contracts in DeFi arrangements, a regulator should evaluate all the facts and circumstances, including: (a) the roles of natural persons and entities in a DeFi arrangement and how those persons and entities interact with each other and how those roles may evolve over time; (b) the ability of those natural persons and entities, such as developers or foundations or decentralized autonomous organizations (DAOs), to control or influence the arrangement, including through actions that would impact a smart contract, protocol, or the enterprise level operations of any particular DeFi arrangement; (c) whether there are other parties exercising control or influence over the DeFi arrangement, such as venture capital firms, large investors, or governance/voting token holders or voters; (d) the economics of the arrangement, including financial incentives for participation, such as who is receiving investments and returns on investment, fees, payments for development or governance activities, or payments from inventories or treasuries; and (e) how a regulator might apply regulatory oversight over these natural persons or entities.[45]

When considering persons and entities that may be Responsible Persons, it is important to note that governance mechanisms currently used for DeFi arrangements are not self-implementing. Human involvement typically is necessary to effectuate governance decisions, or to translate and implement proposals to make changes to a project's protocol, smart contracts or other code into usable code. So those making such proposals often must rely on others with technical control and skill (i.e., administrative access and requisite technical capability) to implement governance decisions. Code could also be designed and updated through the deployment of automated methodologies – including those that utilize artificial intelligence or other technologies. For such cases, the person or entity that is responsible for deploying or using such methodologies could also be considered in the assessment of Responsible Persons. **ANNEX D** gives a detailed analysis of how governance currently operates in DeFi and can be a useful starting point for an analysis.

Depending upon the facts and circumstances, such Responsible Person(s) can include, for example:

- founders and developers of a project;

[45] *Id.* at 27 ("[C]ountries will need to evaluate the facts and circumstances of each individual situation to determine whether there is an identifiable person(s), whether legal or natural, providing a covered service. Marketing terms or self-identification as a DeFi is not determinative, nor is the specific technology involved in determining if its owner or operator is a [Virtual Asset Service Provider (VASP)]. Countries should apply the principles contained in the Standards in a manner that interprets the definitions broadly, but with regard for the practical intent of the functional approach. It seems quite common for DeFi arrangements to call themselves decentralized when they actually include a person with control or sufficient influence, and jurisdictions should apply the VASP definition without respect to self-description. Countries should be guided by the principle that the FATF intends to cover natural or legal persons who conduct the financial services covered in the definition as a business. If they meet the definition of VASPs, owners/operators should undertake ML/TF risk assessments prior to the launch or use of the software or platform and take appropriate measures to manage and mitigate these risks in an ongoing and forward-looking manner.").

- issuers of governance/voting tokens;
- holders and/or voters of governance/voting tokens;
- DAOs or participants in DAOs;
- those with administrative rights to smart contracts and/or a protocol (i.e., with the ability to alter the coding or operation of the protocol to some degree);
- those who have or take on the responsibility of maintaining/updating the protocol or other aspects of the project, such as access rights;
- those with access to material information about the protocol or project to which other participants lack access;
- those who are promoting use of the protocol through, for example, providing a user interface or otherwise facilitating interaction with the protocol, and/or releasing updates to the protocol;
- those with custody (or effective control through an administrative key, voting structure, or otherwise) over user funds or assets, or with the ability to reverse transactions; and
- those who are profiting, for example, through fees paid by users of the protocol.

Once a regulator identifies Responsible Persons, their activities should be assessed using Existing Frameworks or New Frameworks, as appropriate, in accordance with the principle of "same activity, same risk, same regulatory outcome."

Recommendation 3 – Achieve Common Standards of Regulatory Outcomes

A regulator should use Existing Frameworks or New Frameworks to regulate, supervise, oversee, and address risks arising from DeFi products, services, arrangements, and activities in a manner consistent with IOSCO Standards. The regulatory approach should be functionally based to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets.

Guidance

DeFi products, services, arrangements, and activities that involve regulated financial instruments, including securities, in a particular jurisdiction should be subject to applicable laws. Regulators should consider how best to apply their Existing Frameworks or New Frameworks to DeFi products, services, arrangements, and activities. This may include, among other things, IOSCO Standards and laws applicable to issuers, exchanges, trading systems, market intermediaries (including brokers, dealers, investment advisors, custodians, clearing agencies, transfer agents, settlement services, and other service providers), as well as collective investment schemes, hedge funds and other private investment vehicles. The mapping below provides examples of such products, services, arrangements, and activities that may fall within the scope of securities or other financial instrument laws. The mapping in **ANNEX F** details how the IOSCO Standards apply generally to DeFi products, services, arrangements, and activities.

In particular, the regulatory approach relating to DeFi should seek to achieve regulatory outcomes for investor and customer protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets. Regulators should also consider whether existing requirements need to be tailored or adapted to address DeFi-specific features and risks.

- **Investor protection:** A regulator should assess whether their regulatory framework requires material disclosures about DeFi products, services, arrangements, and activities and, if so, who provides them and how. Full, timely and accurate disclosure of material financial and non-financial information provides investors with information about the issuer, the risks and costs of investing in or using a particular DeFi product or service, its governance structure, description of applicable laws, and financial results or other information specific to the DeFi product or service. This may include an analysis of how disclosure standards within the jurisdiction apply to offers/sales of crypto assets in DeFi. A regulator should also assess how their regulatory framework would apply to prevent fraud, misconduct, and other risks to investors, such as those arising from conflicts of interest and interconnectedness.

- **Market integrity:** A regulator should also assess whether their regulatory framework imposes market integrity measures, including those relating to orderly trading with respect to a DeFi product, service, arrangement or activity and, if so, who should provide them and how. To the extent any particular DeFi arrangement (or part thereof) is identified as a CASP, the regulator should apply the recommendations as set forth in the CDA Report accordingly.[46]

As regulators consider to what extent IOSCO Standards and regulatory frameworks within their jurisdiction might apply to particular DeFi products, services, arrangements, and activities, regulators should consider whether they replicate or in fact represent those in traditional finance or whether they are different and, if so, how the features of DeFi, such as technological and operational aspects, may impact the manner of applying existing requirements.

Mapping of Common DeFi Products, Service, Arrangements, and Activities to Traditional Finance

The following mapping may be a helpful starting point for determining what DeFi products, services, arrangements, and activities could fall within the remit of any particular

[46] *See* CDA Report, *supra* note 17.

jurisdiction. For a more detailed explanation of how common typologies in DeFi mimic traditional finance, see the 2022 Report[47] and **ANNEX F** to this report.

Potential Issuers of Financial Instruments, Including Securities: The following are non-exclusive examples of types of DeFi products, services, arrangements, and activities that could involve the issuance of financial instruments, including securities, in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators and DEXs offering and selling their own crypto-assets, including governance tokens, LP tokens or other crypto-assets;
- Lending/borrowing products or services that offer and sell interests in their pools in exchange for crypto-assets. In these cases, market participants deposit crypto-assets into pools in exchange for an interest in the pool. These pool interests are represented by other crypto-assets or tokens that represent the depositor's *pro rata* value of the lending pool. The holder of the pool interest represented by the token can obtain value from it by trading it in secondary markets, borrowing against it, or by presenting it to the pool for redemption of the crypto-asset deposited and all accrued *pro rata* income.
- Lending/borrowing products or services that offer and sell other crypto-assets, such as governance tokens, that may give the holder particular rights, whether to vote on aspects of the lending/borrowing product or service, or other economic interests in the lending/borrowing product or service.
- An AMM or other liquidity pool that offers and sells interests in the pool of crypto-assets that is the AMM. As with the borrowing and lending product tokens that are issued in exchange for crypto-assets deposited in the pools, AMM tokens are also redeemable by the holder for the crypto-asset plus the *pro rata* income from the pool.
- A developer, founder or promotor of DeFi protocols also may directly offer and sell crypto-assets, including in the form of governance tokens, or other crypto-assets. These offers and sales may occur at the initial funding of the protocols or may occur on an ongoing basis with sales of crypto-assets from the treasury of these protocols.
- Aggregators and DEXs also may be involved in offering and selling crypto-assets or tokens of other issuers, thereby participating in distributions of financial instruments, including securities. This may occur through the aggregator or DEX's operations or offerings through which creators or operators of DeFi protocols may distribute governance tokens or other crypto-assets, including crypto-assets that are placed in treasury for distribution.
- The issuance of derivatives, including derivatives/synthetics on traditional financial instruments, as well as the issuance by a cross-chain bridge, wrapping of a token, or in connection with liquid staking.

Potential Market Intermediaries: There are many DeFi products, services, arrangements, and activities that involve market intermediary participants or activities.

[47] 2022 Report, *supra* note 5.

This includes exchange, broker, dealer, investment advisor, custodian, clearing agency, transfer agent, and settlement activities, as well as providers of other services including proxy advisory and credit rating services. The following are non-exclusive examples of types of DeFi arrangements that could involve market intermediary activities in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators, DEXs, and other products and services facilitate the exchange of crypto-assets. DEXs can involve order book exchanges, through which DEXs are performing functions typically associated with exchanges. DEXs can also use AMMs, also known as liquidity pools, which provide liquidity for trading markets. AMMs may be seen to be acting as liquidity providers or market makers thus engaging in buying and selling activities like brokers or dealers.
- Aggregators and DEXs also provide services to users to enable them to trade with multiple AMMs. These activities are akin to broker or dealer activity as well.
- The operation of lending/borrowing products also may involve broker or dealer activity, particularly to the extent that the crypto-assets in the pool are financial instruments, including securities, and the lending product is engaging in lending activities with respect to the crypto-assets that are financial instruments, including securities.
- Each of the AMMs and the lending products may also be engaging in custodial activities and acting as counterparties, due to the manner in which the products engage in holding customer crypto-assets and trading customer crypto-assets. Whether these products and protocols may be acting as custodians of crypto-assets may depend, in part, on how the crypto-assets are transferred to the smart contracts.
- Aggregators enable users to seek the most favorable terms across a variety of protocols. Aggregators allow users to source bids and offers, monitor prices and execute transactions across multiple protocols and trading platforms from a single interface. These activities likely involve exchange, broker or dealer, or investment advisor activity, depending on the particular facts.
- Yield aggregators are platforms of investment opportunities which, depending on how they are structured, provide the functions of either or both a broker and/or an investment advisor. Some yield aggregators provide a type of asset management which has similar characteristics to automated investment or robo-advisory services.
- Portfolio aggregators' primary functionality gives investors visibility into their current positions and allows them to execute transactions from the aggregator's interface thus providing the functions of a broker or dealer.
- Aggregators specializing in governance protocols may centralize proposals and voting across various DAOs, providing recommendations on how to vote on certain proposals. In this capacity, these types of aggregators may be acting as

proxy advisors, if voting is delegated to the protocol. Investors may exchange their voting right(s) for compensation in such arrangements.

- Promotors of DeFi products or services.

Potential Collective Investment Schemes: DeFi products, services, arrangements, and activities may fall within the scope of collective investment schemes (retail/non-retail), hedge funds and other private investment vehicles. Further, DeFi activities and participants that involve operation, marketing, management and advising with respect to these funds may be subject to laws that apply to such activities in many jurisdictions. The following are non-exclusive examples of types of DeFi activities that could involve collective investment schemes (retail/non-retail), hedge funds or other private investment vehicles, and those who operate, market, manage and advise with respect to such funds in certain jurisdictions, or are similar to such activities and participants in others, either currently or in the future:

- Certain aggregators and DEXs may be creating collective investment schemes, hedge funds or other private investment vehicles through the use of AMM arrangements. For example, AMMs typically provide a means for participants to deposit two or more crypto-assets into a smart contract (or liquidity pool) and receive a crypto-asset representing the interest in the pool (and income therefrom). Market participants are then able to use aggregators, DEXs and other service providers to engage in trading activities with the pools. The pools may constitute collective investment schemes. While some of this activity may involve broker or dealer activity, the activity can also include the provision of investment advice. For example, some aggregators provide services that offer investment opportunities to users, such as by obtaining for users the best prices for crypto-assets.

- Lending/borrowing protocols also may involve collective investment schemes, funds and other private investment vehicles. Lending products are pools of crypto-assets deposited by holders in exchange for another token representing the interest in the pool. The lending product then enables other crypto-asset market participants to borrow the crypto-assets in exchange for interest payments. The pooled nature of these lending products may satisfy the definition of collective investment scheme in many jurisdictions. Operators of lending and borrowing protocols also may be viewed, depending on their structures, as investment advisors or sponsors of the collective investment scheme. Initially at least, these operators set the terms of the smart contract arrangements, such as the crypto-asset pairs available to trade, maintain the algorithm to update interest rates, set utilization rates, and address instances of default, including maintenance of a reserve factor.

- Some DeFi products may be structured and operate as hedge funds (or other private funds, or retail/non-retail collective investment schemes), depending on applicable laws. For example, vaults are a mechanism for retail investors to participate in allegedly on-chain *hedge funds* by deploying capital into single or multi-strategy pools run by smart contracts. The sale of the interests in these pools may be collective investment vehicles as they are offered to the public or, if limited to institutions, may be hedge funds. There are also hedge funds that invest or interact with DeFi activities, products and services and the IOSCO Standards applicable to hedge funds would apply to these hedge funds as well.

Potential Exchange/Trading Systems: There are DeFi products, services, arrangements, and activities that could involve exchange and trading system activity. This includes exchange and over the counter activities, both in cash (spot) crypto-asset and derivatives markets. The following are non-exclusive examples of types of DeFi activities and participants that could involve exchange and trading system activity subject to regulation in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators and DEXs facilitate the exchange of crypto-assets. DEXs can involve order book exchanges, through which DEXs are performing functions typically associated with exchanges. DEXs can also use AMMs, also known as liquidity pools, that provide liquidity for trading markets.
- Aggregators and DEXs facilitate the trading of crypto-assets. These activities can involve exchange and trading system activities, and also may operate as an issuer or primary distribution mechanism for new tokens or crypto-assets.
- Aggregators and DEXs also may be acting as a market for derivatives. These kinds of derivatives trading activities include providing protection or selling protection against loss (similar to swaps activities), selling synthetic exposures based on the value of other assets (which could include securities), and engaging in *perpetual futures* trading activity.
- Certain lending/borrowing products may act as exchanges or trading systems depending on the particular structure.
- Many protocols enable automated, and often high-speed, trading, often by sophisticated, well-capitalized entities. Algorithmic trading is common in the DeFi space, and bots are employed to run various trading strategies or identify arbitrage opportunities. Oracles and bridges offer connectivity with off-chain data and between DeFi protocols.

Potential Clearing and Settlement Entities: The following are non-exclusive examples of types of DeFi activities and participants that could involve clearing and settlement activity subject to regulation in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators and DEXs use DLT to transfer ownership of crypto-assets. Depending on the particular protocol, these crypto-assets may be held within an associated smart contract, nominally on behalf of the user of the protocol. Changes in ownership of crypto-assets within DEX and AMMs likely involve clearing and settlement activity.

- Lending/borrowing protocols, as with DEXs and AMMs, generally rely on associated smart contracts to hold crypto-assets and to effectuate transfers of crypto-assets in associated lending pools. Changes in ownership of crypto-assets lending/borrowing protocols likely involve clearing and settlement activity.

- The activities of certain types of aggregators may also be viewed as clearing and settlement activity. For example, yield aggregators are platforms of investment opportunities which, depending on how they are structured, can provide the functions of either or both a broker and/or an investment advisor while potentially acting as a central counterparty. These activities may also operate as settlement systems, depositories, or central counterparties depending on their structure.

- Layer 1 blockchains could themselves be carrying out clearing and settlement activities.

Having undertaken the analysis described above, if a regulator determines that the DeFi arrangement (or any aspect of it) falls within its jurisdictional remit, the regulator should apply its regulatory framework in accordance with the principle of "same activity, same risk, same regulatory outcome."

Regulators may also consider what other laws might apply within their jurisdiction (e.g., data protection, consumer protection, cybersecurity, advertising regulation, legal ownership, etc.) and to what extent they may work with other authorities within their jurisdiction to mitigate risks from DeFi.[48]

Regulators should consider whether applicable frameworks may need to be strengthened, augmented or clarified to address any gaps in applicable frameworks to avoid regulatory arbitrage between traditional financial markets and crypto asset and DeFi markets.

Recommendation 4 – Require Identification and Addressing of Conflicts of Interest

In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to identify and address conflicts of interest, particularly those arising from different roles and capacities of, and products and services offered by, a particular provider and/or its affiliates. These conflicts should be effectively identified, managed and mitigated. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions. This may

[48] Regulators should also assess the AML/CFT risks of DeFi arrangements and require adherence to FATF Standards. *See* FATF, TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 4 (June 2023), available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html ("Jurisdictions should assess illicit finance risks of DeFi arrangements, consider how DeFi arrangements fit into their AML/CFT frameworks, and share their experiences, practices and remaining challenges with the FATF's global network to mitigate the risk of DeFi arrangements.").

include requiring more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.

Many DeFi arrangements and activities today are being conducted in a manner that presents conflicts of interest. DeFi participants may be acting in roles and capacities that create conflicts of interest. Such conflicts can arise, for example, if the provider of a DeFi product or service itself has a financial interest derived from user or third-party activities, an ownership interest in a related third-party, or a favorable arrangement with a particular related party. In particular, the provider may take advantage of their control or influence over the governance of the DeFi arrangement to promote proposals or initiatives that inure to their benefit financially. Conflicts could also arise if the provider is engaged in multiple activities in a vertically integrated matter, either themselves or with affiliated parties. For example, the provider may operate a trading platform while simultaneously being a counterparty to transactions with a user as a market maker or employ technologies like bots or algorithms to transact with users. Indeed, a fundamental conflict may exist if developers, founders and early investors lack the incentive to maintain a project after receiving an initial investment and are instead incentivized to exit the project.

Because of the complexities and opacities in DeFi arrangements, discussed in this report and its Annexes, investors may be unaware that such conflicts may exist. In fact, claims that DeFi is completely transparent due to the public nature of blockchains may mislead investors to believe there are no hidden conflicts, therefore exacerbating risks. Aggressive marketing tactics, behavioral engagement practices, and claims about profitability can further entice investors into arrangements that may put the interests of others over the interests of the investor. These could include the promotion of highly levered strategies or the re-hypothecation of investor assets into a cascade of products and services that may provide benefits to promoters of these strategies in the form of increased fees or kick-backs, for example. It may be unclear to a user the role and capacity in which a provider of a product or service is acting at all times. Concerns around conflicts of interest are further heightened if the provider of the DeFi product or service is in a fiduciary or similar relationship with a user.

A regulator should require Responsible Persons, including providers of DeFi products and services, to be responsible for identifying, managing and mitigating conflicts of interest. A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions, and may require more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions.

A regulator should also seek to require Responsible Persons, including providers of DeFi products and services, to identify, and to the extent practicable, address conflicts of interest that do not directly involve the providers but have an adverse impact on their users/investors.

MEV

There are conflicts of interest that may not directly involve the provider of a DeFi product or service but nevertheless have an adverse impact on the users/investors of the DeFi product or service. One example of such a conflict of interest in the DeFi ecosystem presents itself in connection with certain MEV strategies. Among other things, MEV refers to the exploitation of mempool data[49] by persons or entities participating in a blockchain's consensus mechanism (i.e., miners, validators, or other participants) to maximize their profit by choosing and sequencing proposed transactions from the mempool and/or inserting other transactions that are added to a block to be appended to a blockchain. However, the ability to reorder, insert, and otherwise control transactions enables conduct that in traditional markets would be considered manipulative and unlawful.[50] This activity can result in transactions failing to achieve execution on the terms expected. Such activity could take the form of typical MEV exploits, the most common involving "front-running," "back-running," and "sandwich attacks" (see **ANNEX B**):

- "Front-running" occurs when a participant attempts to execute their own transaction before a pending mempool transaction to realize a profit. A miner/validator could execute this attack through re-ordering transactions on a proposed block or a participant might attempt to pay a higher gas fee or collude with a miner/validator to move their transaction ahead of the pending transaction.[51]
- "Back-running" occurs when a participant seeks to have their transaction executed immediately after a pending transaction. This might be profitable if the pending transaction is to create a new pair for trading on an AMM. An attacker can employ back-running bots that find a new token pair listing and place a transaction order immediately after the initial liquidity to purchase as many tokens as possible, leaving supply in the market depleted.
- A "sandwich attack" is when a participant places two transactions around, one immediately before and another right after, a pending transaction. Searchers typically use sandwich attacks to extract MEV from unsuspecting traders on decentralized exchanges by manipulating the price of an asset. For example, a trader might identify a token that a victim is about to buy and trades to push the price of the asset up, then sells immediately after the victim's buy order has further increased the price.

[49] The mempool consists of transactions that are waiting to be processed by the blockchain's miners/validators.

[50] In certain jurisdictions, these MEV strategies may already be subject to, or prohibited by, existing laws and regulations.

[51] One study calculates the losses due to frontrunning attacks between May 2020 and April 2021 to have amounted to more than $100 million USD. *See* Agostino Capponi et al., *Inefficiencies in Public Distributed Ledgers* (Dec. 31, 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3997796.

- Regulators should seek to hold a provider of a DeFi product or service responsible for identifying and, to the extent practicable, managing and mitigating the impact of MEV strategies used by miners/validators on the underlying blockchain on which the provider chooses to operate or offer the product or service. For example, for a DeFi arrangement that facilitates the trading of regulated financial instruments, the design of the trading mechanism could mitigate the impact of MEV to users/investors trading these instruments. There may be additional conflicts that would need to be addressed if the DeFi product or service provider itself were to have an economic interest in the MEV activity, such as through payment for order flow to certain miners/validators or others.

Recommendation 5 – Require Identification and Addressing of Material Risks, Including Operational and Technology Risks

In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to identify and address material risks, including operational and technology risks. These risks should be identified and effectively managed and mitigated. A regulator should consider whether certain risks are sufficiently acute that they cannot be effectively mitigated and may require more robust measures to address this Recommendation.

A regulator should require providers of DeFi products and services and other Responsible Persons, as appropriate, to establish and maintain a risk management framework that addresses risks arising from the product or service itself, the participants and arrangement, and the market in which the provider of the product or service operates. Where appropriate and consistent with jurisdictional mandates, regulators could impose regulatory requirements to address the risks through means such as the application of "fit and proper" standards.

DeFi arrangements and activities introduce unique operational and technological risks, including those stemming from the underlying DLT, smart contracts and protocols, governance structures, oracles, and bridges. These risks can arise from any one layer of the tech stack that underlies DeFi, as well as from interdependencies between and among those layers of the tech stack. A detailed description of the DeFi tech stack and inherent technological risks can be found in the 2022 Report and in the Annexes to this report. These include, among others, risks arising from the operational interconnectedness of DeFi, due in part to the composability and modularity inherent to DeFi protocols; the proliferation of exploits targeting vulnerable code across protocols' similar code; and a concentration of critical service providers and other participants within DeFi. A regulator should consider how such risks can be identified and effectively managed and mitigated.

Regulators should evaluate, as with other automated or software code based activities in traditional financial products and services, how the automation of certain functions in DeFi arrangements works and consider (a) risks posed by the use of unique or different technology that is not already used in traditional financial markets or otherwise covered by existing regulatory frameworks; (b) how technology, generally, may assist in identifying, managing and mitigating risks in automated products and services; and (c) how regulators may use technology to facilitate supervision and oversight, as appropriate, within a jurisdiction's regulatory framework, and to enhance the IOSCO mandates of investor protection and market integrity.

A provider of DeFi products and services often has control over the smart contracts incorporated into the product or service. A regulator should ascertain what type of control a provider has over a product or service, including through administrative rights to alter smart contracts. A regulator should seek to hold those with control or sufficient influence over the operational or technological features of a DeFi product or service responsible for identifying, managing, and mitigating risks, such as the risk of theft or loss of assets through operational or cybersecurity failures.

A provider of DeFi products and services can rely significantly upon oracles and cross-chain bridges for interoperability with off-chain data or other blockchains. When this is the case, a regulator should consider applying identification, management, and mitigation measures similar to those applied to Responsible Persons in traditional finance, even if certain functionality has been outsourced to affiliated or unaffiliated service providers. In this case, a regulator should consider ways to require the provider to identify, mitigate and manage risk by, for example, requiring adequate due diligence and ongoing monitoring of such service providers, the evaluation, mitigation and management of risks, the implementation of business continuity measures, and the like.[52]

A regulator should consider whether certain risks are sufficiently acute that they cannot be effectively managed or mitigated and may require more robust measures to address this Recommendation.

Oracles and Bridges

Those who provide DeFi products and services often rely on oracles and cross-chain bridges because blockchains essentially operate in siloed environments. Oracles provide connectivity with off-chain data, such as pricing data. Cross-chain bridges provide connectivity with other blockchains. For example, such a bridge can permit a holder of crypto-assets issued on one blockchain to convert to a crypto-asset usable on another, which may facilitate access to liquidity. Such a bridge can also permit the transmission of data between smart contracts of a protocol that is deployed on multiple blockchains, so as to effectuate certain parameter changes to the protocol. However, oracles and bridges present significant technological and operational risks. Those risks are detailed in **ANNEX E**. For example, both oracles and cross-chain bridges have been prone to significant hacks and exploits. One industry report calculates that DeFi protocols lost

[52] *See* IOSCO, PRINCIPLES ON OUTSOURCING (Oct. 2021), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf; *see also* FSB, ENHANCING THIRD-PARTY RISK MANAGEMENT AND OVERSIGHT (June 2023), available at https://www.fsb.org/wp-content/uploads/P220623.pdf.

more than $400 million in 41 separate oracle manipulation attacks in 2022 (see **ANNEX E**), and that 64% of the $3.1 billion stolen from DeFi protocols in 2022 was attributable to cross-chain bridges[53] (see **ANNEX B**).

Regulators should assess whether those providing DeFi products and services present operational and technological risks, including those due to reliance on oracles and cross-chain bridges, among other things. Those risks could be amplified, given particular governance structures that may not be suited to addressing technological and operational risks in a timely and effective manner. Regulators should seek to require providers of DeFi products that rely on oracles and cross-chain bridges to identify, manage and mitigate the risks posed by such technology. In some jurisdictions, regulators may choose to require more robust measures.

Recommendation 6 – Require Clear, Accurate and Comprehensive Disclosures

In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of DeFi products and services and other Responsible Persons, as appropriate, to accurately disclose to users and investors comprehensive and clear information material to the products and services offered in order to promote investor protection and market integrity.

Information about DeFi products, services, arrangements, and activities is often technologically complex and/or opaque. This may arise due to a number of factors, including, but not limited to, the complex nature of the products or services themselves or of the underlying tech stack, and opacities in certain aspects of the arrangement's business, operations and governance. Consequently, the complexity and opacity of DeFi products, services, arrangements, and activities can result in significant information asymmetries, where users and investors are not fully apprised of the nature of the products, services, arrangements, and activities with which they are interacting and the associated risks that they may be exposed to, leading to investor harm.

To address this, a regulator should seek to require providers of DeFi products and services and, as appropriate, other Responsible Persons, to accurately disclose to users and investors comprehensive and clear information about the material aspects of the provider's products, services, business, operations, governance, risks, conflicts of interest, and financial condition. Disclosures should include a plain-language description of material risks to the user or investor. It should also include a description of any crypto-assets involved in the product or service. This may include a prospectus or an equivalent document from an issuer of a crypto-asset or other financial instruments. Disclosure should also include a description of the governance and lines of responsibility and accountability within the DeFi arrangement, including identifying key persons and the roles they play in the provision of the product or service as well as, as appropriate, related parties and outside service

[53] CHAINALYSIS, *supra* note 21, at 58.

providers. Information in marketing and promotional communications should be consistent with such disclosures.

Regulators should require providers of DeFi products and services and other Responsible Persons to disclose any material risks associated with the underlying technologies used to deliver these products and services, as appropriate and in line with jurisdictional legal frameworks.

Recommendation 7 – Enforce Applicable Laws

A regulator should apply comprehensive authorization, inspection, investigation, surveillance, and enforcement powers, consistent with its mandate, to DeFi products, services, arrangements, and activities that are subject to Existing Frameworks and New Frameworks, including measures to detect, deter, enforce, sanction, redress and correct violations of applicable laws and regulations. A regulator should assess what technological knowledge, data and tools the regulator needs to enforce applicable laws.

Guidance

Consistent with the principle of "same activity, same risk, same regulatory outcome," DeFi products, services, arrangements, and activities should be regulated in a manner consistent with the aim of promoting investor protection and preventing the same types of misconduct and fraudulent and manipulative practices that exist in traditional financial markets, as well as any additional risks presented by DeFi. Regulators should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including authorization and licensing requirements, and the ability to undertake inspections or examinations, as appropriate and consistent with their respective mandates. Regulators should seek to bring enforcement actions or other corrective actions against Responsible Persons for fraud and market abuse, in addition to other failures of regulatory compliance, where appropriate. This includes misuse of material, non-public information, insider dealing, market manipulation, issuing false and misleading statements, and misappropriation of funds, among other conduct. The guidance associated with Recommendation 2 can be considered in identifying the appropriate parties that could be held responsible from a regulatory standpoint.

As do other market participants, DeFi market participants may seek to structure their arrangements and activities to avoid regulation, offer products and services within a jurisdiction while operating from another jurisdiction, and/or operate in noncompliance with applicable existing laws, thereby challenging the ability of jurisdictions to regulate, supervise, oversee, and enforce applicable laws, which increases the risk of regulatory arbitrage and weakens investor protections.

In order to address these challenges, regulators should assess whether they have the appropriate powers, tools and resources.[54] Regulators should seek methods to obtain the

[54] Regulators should also consider means to engage and inform investors about DeFi activities and risks, including to enhance investors' understanding of the role of the regulator in relation to DeFi

appropriate data, tools and expertise they will need to conduct investigatory and enforcement activities. This may include crypto-asset market data, including blockchain data, as well as blockchain analytical tools and techniques.

Recommendation 8 – Promote Cross-Border Cooperation and Information Sharing

A regulator, in recognition of the cross-border nature of DeFi products, services, arrangements, and activities, should have the ability to cooperate and share information with regulators and relevant authorities in other jurisdictions with respect to such arrangements, and activities. This includes having available cooperation and information sharing arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorization and on-going supervision of regulated persons and entities and enable broad assistance in enforcement investigations and related proceedings.

Guidance

The owners and operators of DeFi products and services often are based in multiple jurisdictions and/or offer their DeFi products and services on a cross-border basis. Those with control or sufficient influence over the operation of DeFi arrangements can be geographically dispersed across a number of jurisdictions. At the same time, there is often a lack of transparency regarding the ownership and operation of the DeFi products and services, including a lack of available information on the identity and location of the owners and operators of the DeFi protocols and the size and scope of the DeFi arrangements and activities occurring in particular jurisdictions. To the extent that such information is available, the information is often highly complex or technical and/or otherwise limited in some way, including due to the pseudonymous nature of many DeFi activities.

Some DeFi arrangements and activities may claim not to have a geographical location or will claim they have no presence in a particular jurisdiction. Some may point to the fact that they employ a distributed governance structure or that various actors involved in the arrangement or activity are geographically dispersed. Some may choose an organizational structure that is called a *Decentralized Autonomous Organization* or DAO or they may legally organize in one jurisdiction, have personnel in another jurisdiction, and offer products and/or services in yet another jurisdiction. Regulators should consider whether their regulatory framework captures whatever activity is occurring in their own jurisdiction and should consider ways to cooperate with other jurisdictions to the fullest extent practicable in order to address risks to investors and markets within their own jurisdictions.

activities and to provide investors with tools to assess the risks associated with particular DeFi activities and to protect themselves against fraud and other abuses. In so doing, regulators could consider investor education techniques, including those discussed in the IOSCO, RETAIL MARKET CONDUCT TASK FORCE FINAL REPORT (March 2023), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD730.pdf, and in the IOSCO, INVESTOR EDUCATION ON CRYPTO-ASSETS FINAL REPORT (Dec. 2020), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD668.pdf.

Recognizing the cross-border nature of DeFi products, services, arrangements, and activities, regulators should have the ability to cooperate and share information to assist one another to fulfill their respective mandates relating to such products, services, arrangements, and activities. Regulators also should have in place effective cooperation and information sharing arrangements and/or other mechanisms to engage with relevant authorities in other jurisdictions. These should allow regulators to provide broad assistance in enforcement investigations and related proceedings and, as appropriate, the authorization and supervision of regulated DeFi market participants. Cooperation and information sharing should also aim to facilitate a shared understanding of activities and risks of DeFi across jurisdictions. Regulators should aim to share information and cooperate in a timely and effective way, especially when there is a risk of investor or market harm. Regulators should consider ad hoc arrangements to address matters of urgency.

To enhance effective supervision of the markets, regulators should consider bilateral and/or multilateral cooperation arrangements beyond the enforcement context, as appropriate, such as supervisory colleges, networks, regional arrangements, or other forms of cross-jurisdictional cooperation, to support rigorous and effective ongoing supervision of DeFi activities and arrangements operating across multiple jurisdictions.

Regulators should cooperate with each other and share information, both domestically and internationally, consistent with their respective mandates and applicable legal requirements and, to the greatest extent possible, to promote effective information sharing to assist one another with fulfilling their respective mandates and, where appropriate, to encourage the consistency of outcomes relating to DeFi, including cooperation and information sharing in the following areas:

- **Emerging Risks:** Regulators should cooperate and share information relating to DeFi activities occurring across jurisdictions, for effective risk monitoring of DeFi activities, and to facilitate a shared understanding of related risks, including to market integrity, investor protection, and financial stability. In particular, regulators should share information on emerging trends and other developments with the potential for significant cross-border impacts, as well as information to assist with understanding and analyzing DeFi arrangements (i.e., in furtherance of these Recommendations). Sharing typologies of DeFi arrangements and activities, as appropriate, may also assist in analyzing and comparing observed behavior.

- **Registration/Authorization:** Regulators should cooperate and share information relating to requests by other regulators regarding firms engaged in DeFi activities to become registered and/or authorized to conduct business in a particular jurisdiction, for example, as a type of trading venue authorized within a particular jurisdiction. Among other things, regulators should have the ability to share information relevant to the requesting regulator's decision whether to register and/or authorize such firms, provided that any confidentiality requirements are satisfied. Examples of information that should be shared may include the ownership and operation of the DeFi products and services in which the firm is engaged, and other relevant features of the DeFi activities of the firm, including the size and scope of the DeFi products and services offered by the firm and the firm's compliance with relevant applicable laws and regulations across jurisdictions.

- **Supervision:** Regulators should also seek to enable cooperation and information sharing to further the effective supervision of DeFi activities, consistent with their respective jurisdictions' laws and regulations. Regulators should use existing cooperation and information sharing arrangements (e.g., memoranda of understanding, ad-hoc arrangements, supervisory colleges, networks), to the fullest extent practicable, or consider establishing new bilateral or multilateral cooperation and information sharing arrangements that may encompass additional subject areas or jurisdictional authorities, to support the effective ongoing supervision of DeFi activities operating across multiple jurisdictions. Regulators should utilize such arrangements to provide assistance to one another with, among other things, examinations and inspections of registered firms engaged in DeFi activities, including to provide other regulators with access to the books and records of those firms, if appropriate.

- **Enforcement:** IOSCO has in place effective mechanisms for cross-border cooperation between financial market authorities to enable the enforcement of laws and regulations applicable to DeFi. Information requests relating to DeFi are captured by IOSCO's Multilateral Memorandum of Understanding (MMoU)[55] and Enhanced Multilateral Memorandum of Understanding (EMMoU)[56], premised on the underlying principle of "same activity, same risk, same regulatory outcome." Regulators should use the MMoU and EMMoU to the greatest extent possible to enable cooperation and information sharing relating to DeFi activities. Beyond the MMoU and EMMoU, regulators should also share information with one another and, where relevant, with law enforcement authorities, and work together to stop abusive and criminal behaviors, including financial crime and money laundering, and to mitigate risks to investors.

Recommendation 9 – Understand and Assess Interconnections Among the DeFi Market, the Broader Crypto-Asset Market, and Traditional Financial Markets

When analyzing DeFi products, services, arrangements, and activities, a regulator should seek to understand the interconnections among DeFi arrangements, the broader crypto-asset market, and also the traditional financial markets. In so doing, a regulator should consider how those interconnections impact risks to

[55] IOSCO, MULTILATERAL MEMORANDUM OF UNDERSTANDING CONCERNING CONSULTATION AND COOPERATION AND THE EXCHANGE OF INFORMATION (rev. May 2012), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD386.pdf.

[56] IOSCO, ENHANCED MULTILATERAL MEMORANDUM OF UNDERSTANDING CONCERNING CONSULTATION AND COOPERATION AND THE EXCHANGE OF INFORMATION (2016), available at https://www.iosco.org/about/pdf/Text-of-the-EMMoU.pdf.

investor protection and market integrity, and how they might identify further regulatory touchpoints, including potential responsible persons. A regulator should, as appropriate, seek to employ, maintain and develop suitable methods for monitoring and assessing DeFi products, services, arrangements, and activities.

Guidance

The 2022 Report discussed the importance of centralized crypto-asset trading, lending and borrowing platforms and stablecoins to DeFi. Specifically, centralized platforms are often the on-ramp to participation in DeFi, including by retail investors, and stablecoins facilitate participation in DeFi arrangements, serving as the perceived stable value asset used as one side of a trading pair, or in liquidity or collateral pools to fund or collateralize DeFi activities. Thus, events (such as liquidity crises) that cause shocks or disruptions on centralized platforms or to stablecoins likely will impact DeFi markets. Indeed, some recent crypto-asset market events and their impact on DeFi are discussed in **ANNEX A**. Regulators should consider how interconnectedness within the crypto-asset markets will impact investor protection and market integrity in DeFi markets. Regulators should also consider whether steps should be taken with respect to centralized platforms and stablecoins and to adhere to the recommendations and guidance contained in the CDA Report[57] to provide additional investor and market protections.

Regulators should consider how regulatory touchpoints in the DeFi market, the broader crypto-asset market, and traditional financial markets could provide information and, where appropriate, regulators should require the relevant Responsible Persons to apply investor and market protections. Regulators should consider ways to identify these touchpoints, including through surveys of registered entities or through other regulatory frameworks, such as those that pertain to anti money laundering (AML)/countering the financing of terrorism (CFT).

Regulators should understand and assess risks relating to the exposures of traditional financial market participants (i.e., existing regulated entities) to DeFi structures (e.g., through hedge funds, private equity funds, intermediaries, broker or dealers, investment advisers, transfer agents, clearing agencies, custodians, and other institutional participants). Regulators should consider additional approaches to provide important investor, customer and market protections for DeFi market participants, including through their regulation and oversight of traditional financial market participants or centralized crypto-asset platforms involved, directly or indirectly, in DeFi arrangements or activities.

Given the potential effects of DeFi on TradFi, it is important to be able to monitor and evaluate interlinkages between DeFi and traditional financial markets. The following outlines some ways that crypto-assets could touch traditional entities, though these are not exhaustive of all types of connectivity:[58]

[57] CDA Report, *supra* note 17.

[58] *See also* FSB DeFi Report, *supra* note 12, at 25-26; BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 15 (July 2023), available at https://www.bis.org/publ/othp72.pdf ("[R]isks along the bank-crypto nexus extend beyond (direct and indirect) exposures because of the potential negative externalities

Entity		Potential Relationship to DeFi
Issuer of financial instrument, including securities		Issue crypto-asset; engage in crypto-asset-related operational activities (e.g., mining/validating); hold crypto-assets (e.g., in corporate treasury); participate in governance
Funds (registered)		Invest in DeFi related investments or have exposure to DeFi products/services; participate in governance
Broker/dealer/investment adviser		Conduct services relating to DeFi products/services; link customers to DeFi products/services
Banks/trusts/money services businesses/credit card issuers		Provide services relating to DeFi products/services; invest in DeFi products/services; link customers to DeFi products/services
Third party service providers (auditors/accountants/transfer agents/credit rating entities)		Provide services to DeFi products/services

Regulators should assess potential data sources to monitor interconnections with traditional markets. Such data or indicators might pertain to:

- Traditional financial services being provided to DeFi participants (i.e., banking, loans, holding or managing reserves, fiat to crypto-asset exchange, etc.)
- Correlations between crypto-assets and certain traditional assets (and changes over time)[59]

associated with banks channeling funds into the crypto ecosystem, given their role as the mainstay of the monetary system. Along with banks, other financial entities such as family offices, hedge funds and asset managers could also increase their crypto investments, lured by the potentially high returns.").

[59] *See* Tara Iyer, *Cryptic Connections: Spillovers between Crypto and Equity Markets*, GLOBAL FIN. STABILITY NOTES No 2022/001 (Jan. 11, 2022), https://www.imf.org/en/Publications/global-financial-stability-notes/Issues/2022/01/10/Cryptic-Connections-511776.

- Spillovers between crypto-asset prices and select traditional assets (and changes over time) (e.g., computed by the application of econometric models)[60]
- Size/reserves of stablecoins
- VC/private institutional investment in crypto-assets
- Derivative/synthetic exposure to crypto-assets
- Crypto-assets that are derivatives/synthetics of real-world assets
- The use of real-world assets as collateral or components in DeFi activities

[60] *Id.*

SECTION IV. QUESTIONS FOR PUBLIC CONSULTATION

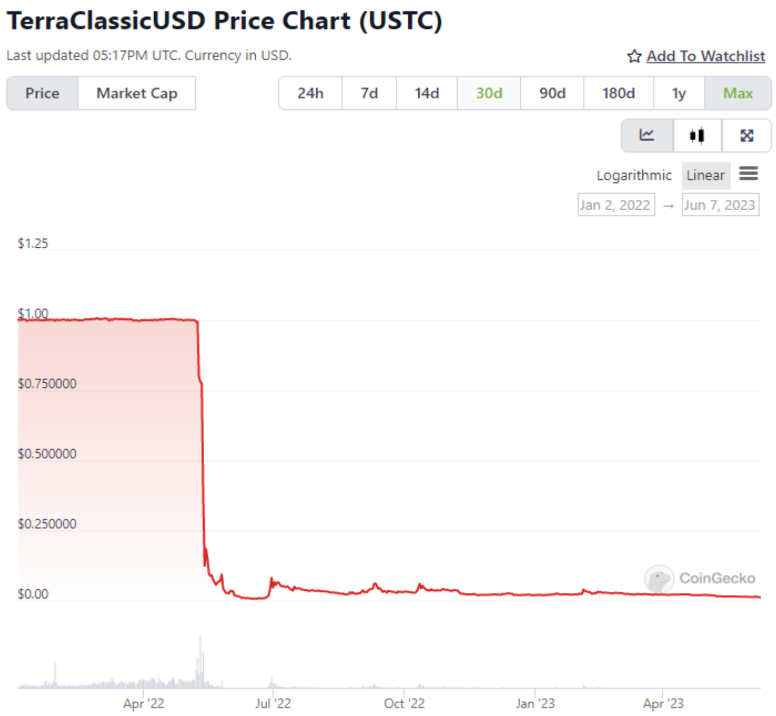
1. Do you agree with the Recommendations and guidance in this Report? Are there others that should be included?
2. Do you agree with the description of DeFi products, services, arrangements, and activities described in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details.
3. Do you agree with the Report's assessment of governance mechanisms and how they operate in DeFi? If not, please provide details.
4. Do you agree with the risks and issues around DeFi protocols identified in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants help address these risks and/or issues, including through the use of technology? How would you suggest IOSCO members address these risks and/or issues?
5. Do you agree with the description of data gaps and challenges in the Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants address these data gaps and challenges, including through the use of technology? How would you suggest IOSCO members address data gaps and challenges?
6. Do you agree with the application of IOSCO Standards to DeFi activities contained in this Report? Are there other examples of how IOSCO Standards can apply?
7. Is there any additional guidance that you would find relevant to help IOSCO members comply with these Recommendations? If so, please provide details.
8. Given the importance of the application of IOSCO Standards to DeFi activities, are there technological innovations that allow regulators to support innovation in DeFi/blockchain technologies while at the same time addressing investor protection and market integrity risks? If so, please provide details.
9. Are there particular methods or mechanisms that regulators can use in evaluating DeFi products, services, arrangements, and activities, and other persons and entities involved with DeFi? If yes, please explain.
10. Do you find the interoperability between this report and the IOSCO CDA Report to be an effective overall framework? If not, please explain.

ANNEX A – RECENT EVENTS[61] AND THEIR IMPACT ON DEFI

Terra USD (UST)/LUNA Collapse

Event Summary:

Over the course of several days in May 2022, the value of Terraform Labs' algorithmic stablecoin, Terra USD (UST), and native token of the Terra blockchain (LUNA), both collapsed, erasing nearly $40 billion in reported total market value. The price of UST began to depeg from $1 on May 7, 2022, falling to approximately $0.37 on May 12, 2022, while the price of LUNA, which was purported to be used to stabilize UST's price, fell from approximately $119 in April 2022, to a few cents by May 12, 2022.[62]



TerraClassicUSD Price Chart (USTC)

Last updated 05:17PM UTC. Currency in USD.

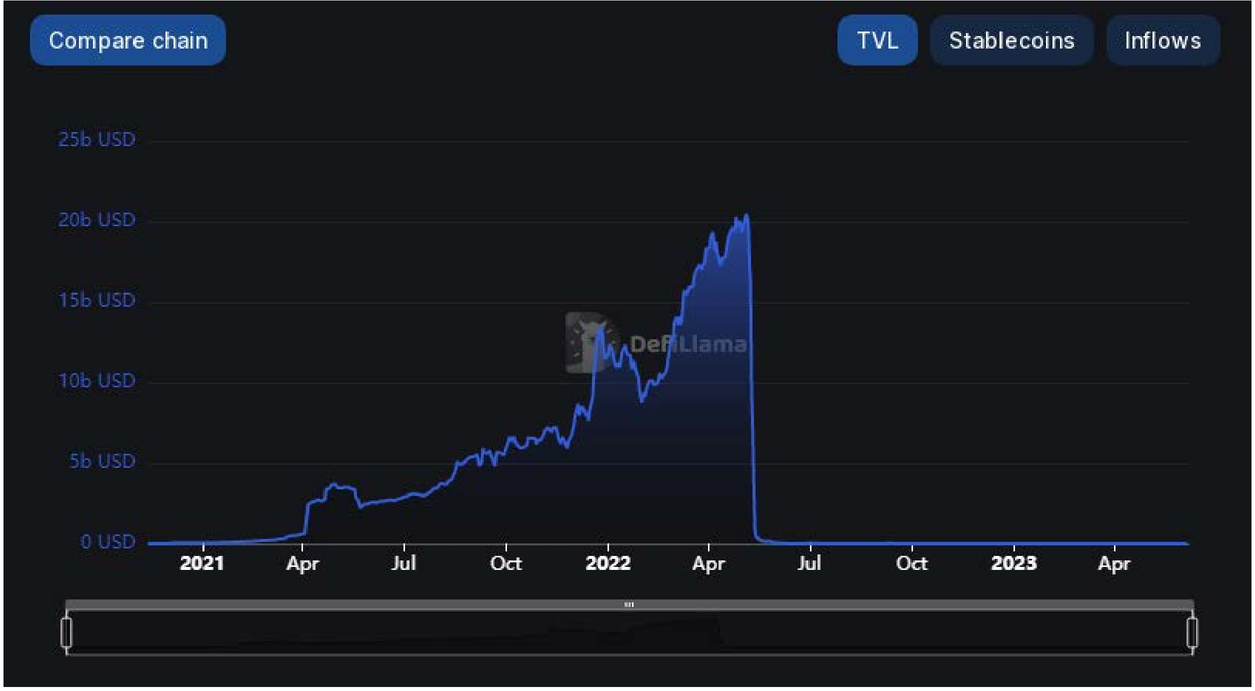
Source: CoinGecko

[61] This report refers to specific recent events as examples. Use of these examples in the report does not constitute any claim about compliance or non-compliance of any particular crypto-asset, person or entity with existing laws and regulations in relevant jurisdictions. Individual jurisdictions might have different legal interpretations of terms used in this report and different views of compliance or non-compliance of the mentioned crypto-assets, persons or entities with laws and regulations relevant to these jurisdictions. All factual descriptions of crypto-assets, persons and entities are based on information currently known to the authors of this report and are subject to change and revision if new information arrives.

[62] The U.S. Securities and Exchange Commission filed an enforcement action against Terraform Labs PTE Ltd. and its founder, Do Hyeong Kwon, on February 16, 2023. *See* https://www.sec.gov/litigation/complaints/2023/comp-pr2023-32.pdf.

Impact to DeFi Market:

In the weeks after UST lost its $1 peg, billions of dollars worth of crypto-assets reportedly were taken out of the Terra ecosystem. The TVL of DeFi applications on the Terra blockchain dropped from approximately $20 billion on May 5, 2022 to less than $75 million on May 28, 2022. This includes the "Anchor" protocol associated with Terra, which had TVL of more than $16 billion at its peak.

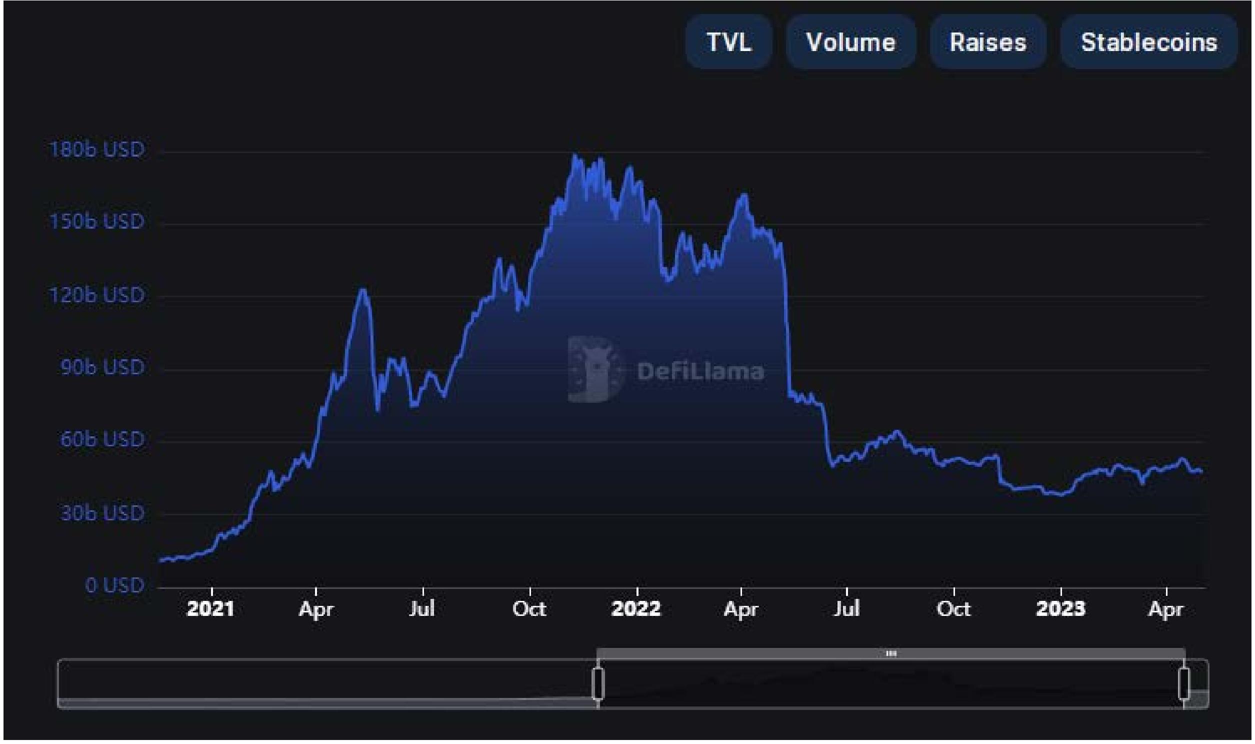


Source: DeFiLlama

The Terra blockchain was halted during this period, preventing users from conducting transactions, while validators and developers reportedly were coordinating activities. In the broader DeFi ecosystem, the death spiral of UST and LUNA appears to have caused a contagion effect, impacting the overall TVL across DeFi platforms on various blockchains. This resulted in a decline from approximately $142 billion on May 5, 2022, to less than $80 billion on May 13, 2022, for a TVL loss of nearly 44% in less than two weeks. One research paper suggests that the existence of bridges between the Terra blockchain and other blockchains exacerbated the impacts of the Terra collapse across DeFi, finding that "bridges between programmable blockchain networks create increased risk of spillover effects to other blockchains' programmable environments in the wake of a major shock event like Terra's collapse."[63] The rapid decline in TVL on the Terra blockchain was seen to demonstrate, among other things, the risks of algorithmic stablecoins, the reality that a blockchain can be halted where no user may thereafter transact or exit their positions when desired, and the impact of sentiment and confidence of DeFi market participants on DeFi

[63] *See* https://www.federalreserve.gov/econres/feds/files/2023044pap.pdf.

arrangements and activities. In particular, it would appear that the performance of crypto-assets native to a blockchain or DeFi arrangement is linked to their overall credibility.[64]



Source: DeFiLlama

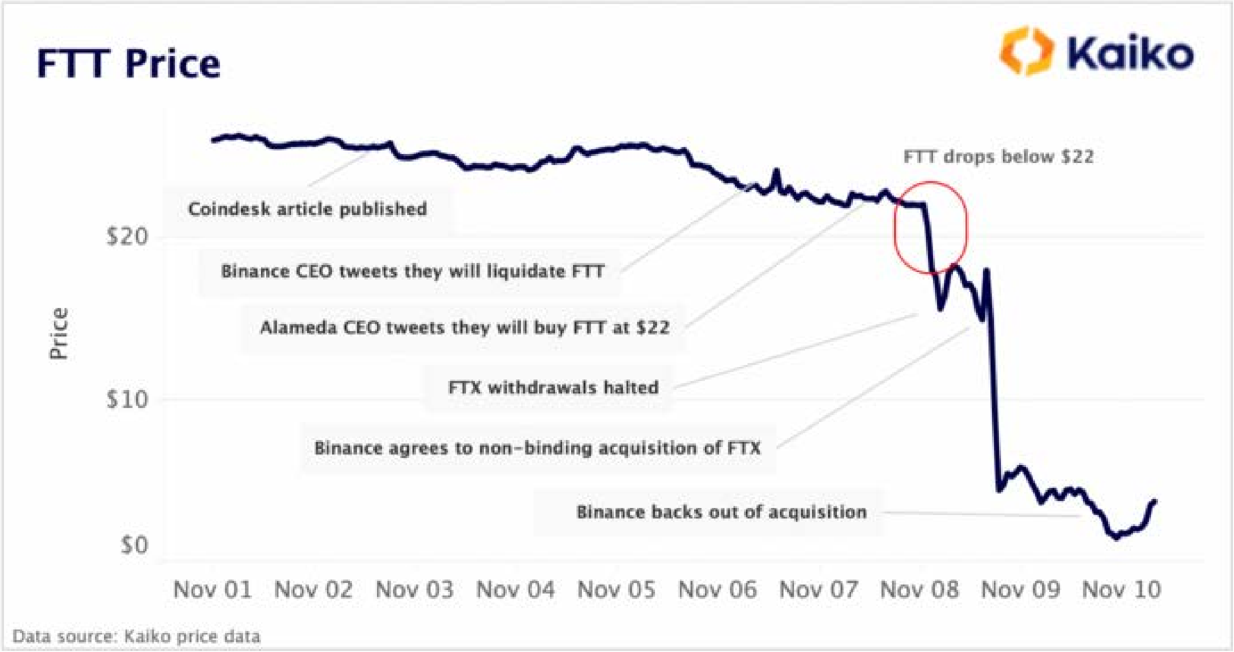
FTX Insolvency

Event Summary:

On November 2, 2022, an article was published, stating that FTX, at the time one of the largest centralized crypto-asset trading platforms by trading volumes, recorded on its balance sheet a significant amount of the *exchange token* of the FTX trading platform (FTT) that purportedly gave certain benefits to holders. Subsequently, the CEO of Binance Holdings Limited (Binance) announced on November 6, 2022, that Binance would liquidate its FTT holdings, which reportedly began a bank-like run as FTX customers apparently lost confidence in the solvency of FTX. FTX reportedly suffered a liquidity crisis, halted customer withdrawals on November 8, 2022, and declared bankruptcy on November 10, 2022.[65]

[64] *See also* BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 7 (July 2023), https://www.bis.org/publ/othp72.pdf (noting that the Terra collapse highlights "the tendency to fragmentation through crypto's vulnerability to new entrants who prioritise market share and capacity and the expense of decentralisation and security.").

[65] The events leading to FTXs insolvency are the subject of on-going civil and criminal actions. *See, e.g.*, https://www.sec.gov/news/press-release/2022-219; https://www.cftc.gov/PressRoom/PressReleases/8638-22; https://www.justice.gov/usao-sdny/pr/united-states-attorney-announces-charges-against-ftx-founder-samuel-bankman-fried.



Source: Kaiko

Impact to DeFi Market:

The collapse of FTX appears to have led to wider contagion in the crypto-asset markets, in which market participants suffered losses. Among those impacted were customers, both retail and institutional, with funds on FTX, counterparties to FTX, investors in FTX and FTT, and others. Although FTX was a centralized crypto-asset platform, this contagion appears to have spread to the DeFi ecosystem. FTX and its principal reportedly were major promoters of the Solana blockchain and its ecosystem.[66] One particular DeFi protocol built on Solana reportedly required a hard fork because FTX purportedly owned the private key to the protocol. The contagion from FTX also appears to have affected a number of other platforms through financial interlinkages, such as lending platforms and a crypto-asset related investment fund.[67] The investment fund reportedly was a participant in a DeFi lending pool run by a delegate firm on a given DeFi protocol that underwrote loans on the protocol. As a result of the investment fund's default, other participants in the lending pools were reported to have suffered losses, including an insurance protocol and a smart contract auditing platform. Further, there was an increase in DeFi transaction volumes, potentially due to the inability to use FTX and other lending platforms and/or a loss of confidence in centralized crypto-asset platforms. Due to the pseudonymity of DeFi

[66] *Life After FTX: How Solana DeFi Is Starting Over—Without SBF's Serum*, YAHOO! NEWS, Dec. 7, 2022, https://news.yahoo.com/life-ftx-solana-defi-starting-223848156.html.

[67] *A Hedge Fund Hit by FTX Collapse Defaults on $36 Million of Debt*, BLOOMBERG, Dec. 6, 2022, https://www.bloomberg.com/news/articles/2022-12-06/crypto-fund-orthogonal-defaults-on-36-million-debt-as-ftx-contagion-spreads?utm_source=website&utm_medium=share&utm_campaign=copy.

participants, it remains a complex challenge to proactively identify participants and their potential interlinkages and concentration risks.

BUSD Minting Cessation

Event Summary:

On February 13, 2023, the New York State Department of Financial Services (NYDFS) ordered Paxos Trust Company (Paxos) to cease minting Paxos-issued Binance USD ("BUSD").[68] In response, Paxos informed its customers of its intent to end its relationship with Binance for BUSD.[69] Prior to the NYDFS cease-minting order, Paxos had been authorized by NYDFS since September 2019 to offer BUSD subject to the conditions that all Paxos-minted BUSD on the Ethereum blockchain be backed by cash, short term treasuries, and other highly liquid investments on a 1:1 basis as well as be subject to other regulatory requirements.[70] NYDFS stated that all US residents who own Paxos-minted BUSD could still exchange BUSD at a 1:1 rate for US dollars even after the cease-minting order. NYDFS also stated that its prior approval order to Paxos authorized only BUSD on the Ethereum blockchain, noting it had not authorized the Binance-Peg BUSD, a wrapped version of BUSD, purportedly designed to track the value of BUSD at a 1:1 ratio.[71] Approximately one month later on March 13, 2023, the CEO of Binance announced that Binance was converting $1 billion of BUSD to BTC, ETH and BNB (the "exchange token" of the Binance platform).

Impact to DeFi Market:

Concurrent to the February 13, 2023, announcements by NYDFS and Paxos, the reported total TVL across DeFi rose by approximately 7% over a three day period ending on February 16, 2023, from approximately $46 billion to more than $49 billion, the highest level since the first week of November 2022, shortly before the collapse of FTX. Simultaneously, investors reportedly withdrew approximately $2.3 billion worth of BUSD from Binance within four days of the NYDFS announcement.

The NYDFS supervisory action relating to BUSD may have impacted the willingness of certain DeFi market participants to use BUSD. Participants in Curve's busdv2 liquidity pool exchanged BUSD for the two other pool components, USDT and DAI,[72] to such an extent

[68] *See* https://www.dfs.ny.gov/consumers/alerts/Paxos_and_Binance.

[69] *See* https://paxos.com/2023/02/13/paxos-will-halt-minting-new-busd-tokens/.

[70] *See* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1909051.

[71] *See* https://www.binance.com/en/blog/ecosystem/understanding-busd-and-binancepeg-busd-5526464425033159282.

[72] DAI purports to be a crypto-asset-collateralized stablecoin pegged to USD that is maintained and regulated by MakerDAO. *See* https://makerdao.com/whitepaper/DaiDec17WP.pdf.

that on February 14, 2023, 81% of the assets in busdv2 were BUSD.[73] Market participants reportedly experienced intense selling pressure and price slippage.[74] Both centralized exchanges[75] and DeFi protocols[76] reportedly limited the use of BUSD. The impact of these actions by NYDFS and Paxos illustrate, among other things, certain risks of stablecoins. In this particular instance, for example, Binance reportedly was minting BUSD on a non-Ethereum blockchain without consistently maintaining a 1:1 reserve rate. These events also illustrate how investors may tend to migrate assets from a centralized platform to DeFi when they lose confidence in the centralized platform, how investors may tend to avoid crypto-assets against which regulatory or supervisory actions have been commenced, the high impact certain events can have on liquidity and transaction fees on DeFi platforms, and the ability of purported "decentralized" DeFi platforms to freeze or restrict certain products or assets when certain risks arise.

USDC Depeg

Event Summary:

In 2023, the failure of a US regional bank that offered deposit services to a stablecoin issuer contributed to a temporary de-pegging of its stablecoin because of uncertainty about the issuer's access to its deposits.[77]

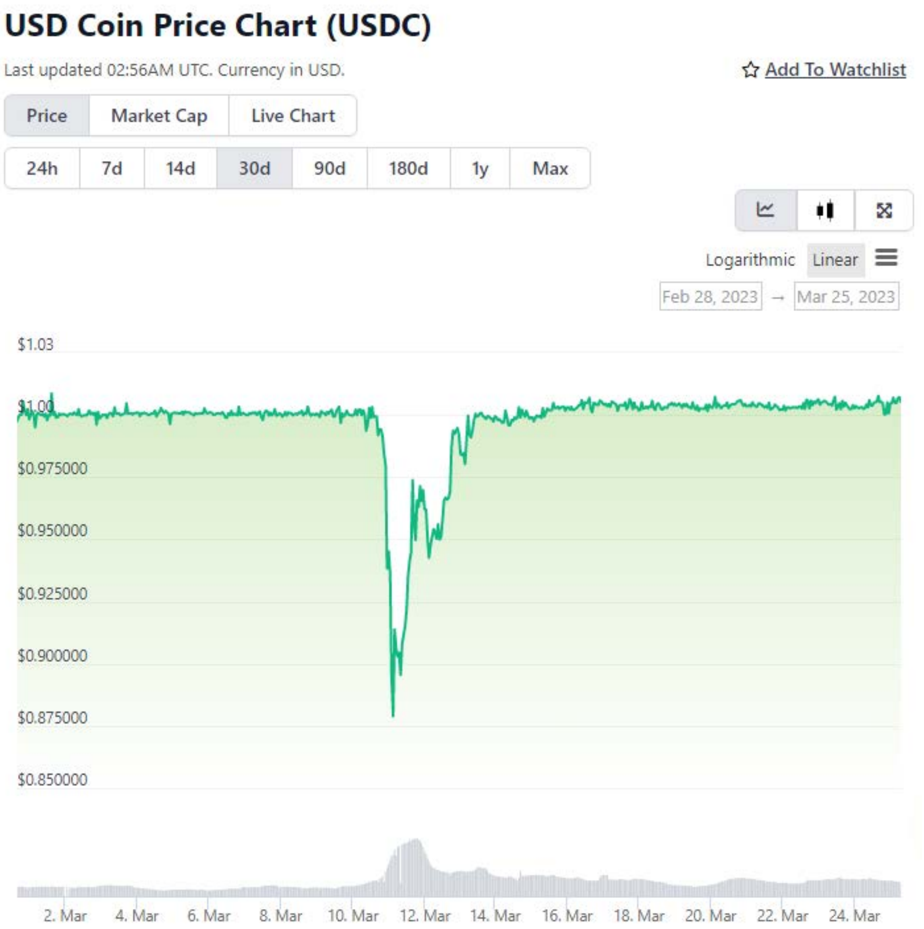
[73] Omkar Godbole, *Investors Rush to Tether as Paxos' BUSD Faces Regulatory Heat, Curve Liquidity Pools Show*, COINDESK (Feb. 14, 2023, 7:29 am), https://www.coindesk.com/markets/2023/02/14/investors-rush-to-tether-as-paxos-busd-faces-regulatory-heat-curve-liquidity-pools-show/?ref=biztoc.com.

[74] *See, e.g.*, Tiny Cat (@insigocelot), TWITTER (Feb. 13, 2023, 7:57 AM), https://twitter.com/insigocelot/status/1625116840782442498 ("And just like that defi exit liquidity for BUSD was gone. Only significant remaining pool of BUSD liquidity remaining is on Pancake Swap. All stable pools on Ethereum thoroughly dumped. A $1,000,000 sale of BUSD on Uni now subject to 35%+ slippage."); @Mr. Kazoo Bitcoin, TWITTER (Feb. 14, 2023, 4:52 AM), https://twitter.com/MrKazooBitcoin/status/1625432771660500992 ("You need to pay +$30 to buy 1 $BTC on #BUSD market, the slippage is real 😕").

[75] Oliver Knight, *Coinbase Officially Suspends Binance USD Stablecoin Trading*, COINDESK (Updated May 9, 2023, 12:10 am), https://www.coindesk.com/business/2023/03/13/coinbase-officially-suspends-binance-usd-stablecoin-trading/#:~:text=Cryptocurrency%20exchange%20Coinbase%20(COIN)%20has,Brian%20Armstrong%20citing%20liquidity%20concerns.

[76] Samuel Haig, *Aave and Maker Pull Back From Paxos Stablecoins*, THE DEFIANT, Feb. 21, 2023, https://thedefiant.io/aave-and-maker-pull-back-from-paxos-stablecoins.

[77] *See* FSB, GLOBAL REGULATORY FRAMEWORK FOR CRYPTO-ASSET ACTIVITIES 4 (July 2023) available at, https://www.fsb.org/2023/07/fsb-global-regulatory-framework-for-crypto-asset-activities/; CIRCLE, USDC RESERVE REPORT (Jan. 2023), available at https://www.circle.com/hubfs/USDCAttestationReports/2023%20USDC_Circle%20Examination%20Report%20January%202023.pdf.



USD Coin Price Chart (USDC)

Last updated 02:56AM UTC. Currency in USD.

Feb 28, 2023 → Mar 25, 2023

Source: CoinGecko

<u>Impact to DeFi Market:</u>

Given the common use of stablecoins as one leg of a trading pair in many DeFi protocols, USDC's depeg had systemic impacts across DeFi. DeFi pools such as Curve's 3pool (where each crypto-asset typically represents 33% of the pool's value) experienced an initial flight from USDC.[78] Tether (USDT) gained notable inflows following the 3pool USDC flight.[79]

In the wake of these events, a number of DeFi projects made or passed governance or DAO proposals to address USDC risk. For example, MakerDAO launched an emergency proposal

[78] *See* Danny Nelson, *DeFi Protocol Curve's $500M Stablecoin Pool Hammered as traders Flee USDC*, COINDESK (Updated May 9, 2023, 10:10am), https://www.coindesk.com/business/2023/03/10/defi-protocol-curves-500m-stablecoin-pool-hammered-as-traders-flee-usdc/.

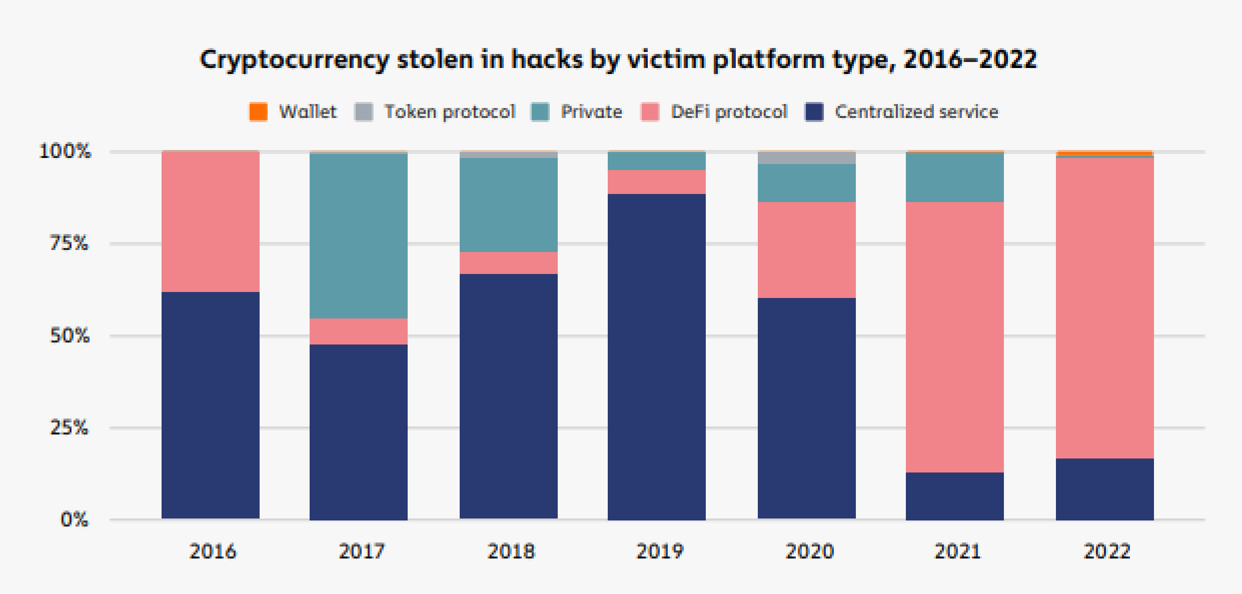
[79] Krisztian Sandor, *USDC Outflows Surpass $10B as Tether's Stablecoin Dominance Reaches 22-Month High*, COINDESK (Updated Mar. 30, 2023, 3:55 pm), https://www.coindesk.com/markets/2023/03/29/usdc-outflows-surpass-10b-as-tethers-stablecoin-dominance-reaches-22-month-high/.

to change its risk parameters to reduce exposure to USDC.[80] This proposal appears to have been proposed and passed in roughly eight hours. The USDC depeg illustrates, among other things, interconnectedness between fiat-based stablecoins and the banking sector and the existence of contagion channels between TradFi and DeFi. The USDC depeg also illustrates the risks to participants using stablecoins as collateral in DeFi arrangements. The events also suggest that DeFi participants use elevated rights and exceptions to stated governance processes in DeFi to respond to events that cause market stress or increase risks to a DeFi arrangement or activity.

[80] *See* https://cointelegraph.com/news/maker-dao-files-emergency-proposal-addressing-3-1b-usdc-exposure; https://forum.makerdao.com/t/emergency-proposal-risk-and-governance-parameter-changes-11-march-2023/20125.

ANNEX B – DEFI EXPLOITS, ATTACKS AND ILLICIT USES

The DeFi markets, like other financial markets, are a target for hackers and attackers, including those that seek to exploit vulnerabilities to misappropriate funds and data. This section describes various attacks and specifically highlights flash loan- and Maximal Extractable Value (MEV)-enabled attacks.[81] According to one blockchain analytics firm, attacks on DeFi protocols accounted for 82.1% of all crypto-assets stolen by hackers in 2022— a total of $3.1 billion — up from 73.3% in 2021. Of that $3.1 billion, 64% was attributable to attacks on cross-chain bridges.[82] Another blockchain analytics firm reported that nine of the ten largest attacks occurred against DeFi projects,[83] and that hacks on such projects resulted in an average of more than $20 million stolen per incident.[84]



Source: Chainalysis – The 2023 Crypto Crime Report

A blockchain analytics firm reports that among the most prolific hacker groups are those associated with North Korea. Reportedly, the North Korea-linked Lazarus Group stole an estimated $1.7 billion worth of crypto-assets in 2022, and North Korea-linked hackers have stolen $1.1 billion in crypto-assets through hacks of DeFi protocols. The report

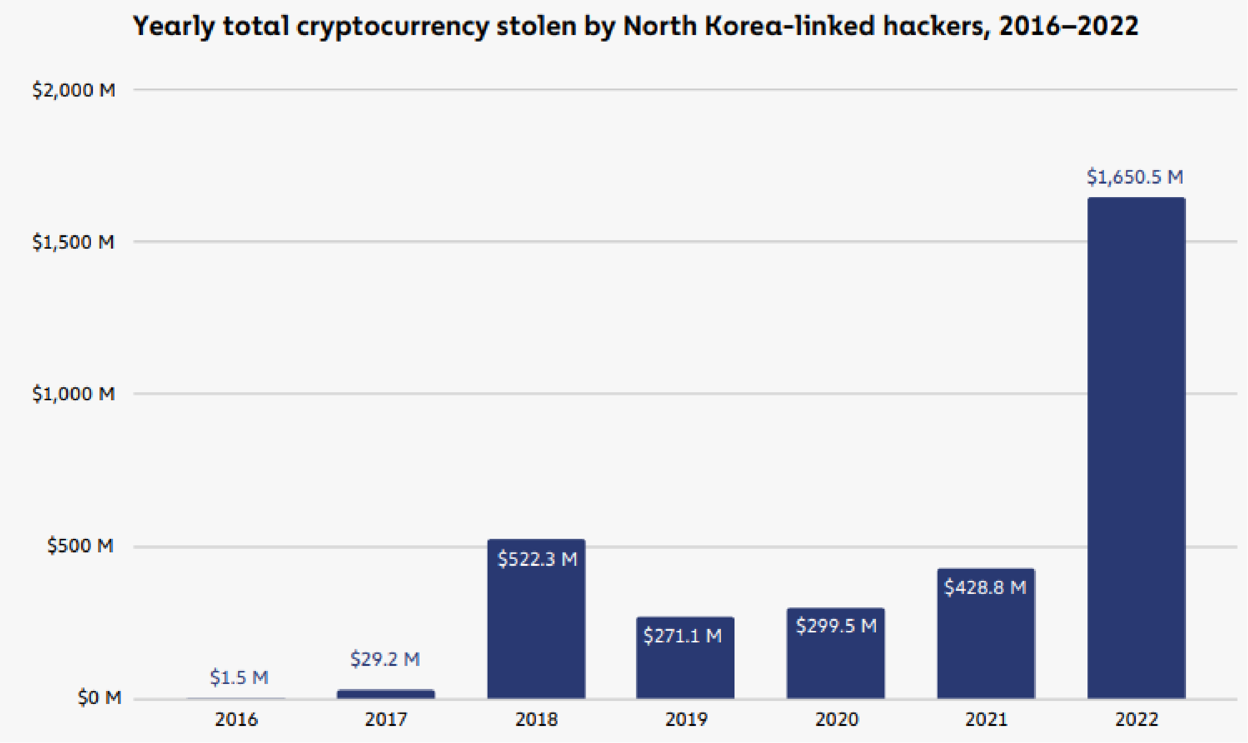
[81] This section does not cover market manipulation and outright scams. *See, e.g.*, IOSCO, RETAIL MARKET CONDUCT TASK FORCE FINAL REPORT (Mar. 2023), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD730.pdf. Each of these, however, is a significant source of risk.

[82] CHAINALYSIS, *supra* note 21.

[83] TRM, *supra* note 22, at 32.

[84] *Id.* at 52.

concludes that the funds are laundered through DeFi protocols in order to convert stolen crypto-assets into more liquid or less volatile assets before eventually being converted to fiat currencies at centralized crypto-asset platforms.[85]



Source: Chainalysis – The 2023 Crypto Crime Report

Common Types of Exploits/Attacks

Common types of exploits and attacks observed in DeFi are discussed below. Of note, most attacks have exploited one or more features of DLT-based systems, namely:

- Public, open-source code, which makes it possible for threat actors to study a protocol's smart contracts and test how it may be exploited;
- DeFi governance structures;
- Private keys, which in some cases can control significant functionality of a smart contract through elevated or administrative functions that allow any holder of those keys to commandeer crypto-assets. Private keys are susceptible to compromise through common cyberattacks, such as phishing, key logging or social engineering;
- Permissionless access, which makes it possible for anyone with the necessary technical skills to interact with any protocols of their choice; and
- The fact that code is often copied and used in multiple protocols, which can exacerbate an attack as it can be carried out across multiple protocols.

[85] CHAINALYSIS, *supra* note 21.

Exploits and attacks in DeFi target vulnerabilities inherent to DeFi arrangements, such as smart contract code or dependencies on critical infrastructure (e.g., oracles, bridges). Threat actors investigate publicly accessible code, and also use tools and techniques such as flash loans and MEV to effectuate an attack. The following discusses vulnerability-related targets for exploits and tools used to carry out attacks.

Smart Contract-Related

Smart contracts are code that is deployed on a blockchain or DLT-based system and form the major building blocks of DeFi protocols. Just as with other software, smart contracts are susceptible to code errors and vulnerabilities, and have proven a major attack vector for DeFi exploits. What are often seen as features of smart contracts (e.g., the fact that they can be self-executing, immutable, composable, and can be publicly inspected) also can translate to vulnerabilities in terms of an attack vector.

One major type of exploit relates to access control, which involves using a smart contract's private key(s) to alter the smart contract in some way. With access to a private key that can sign elevated administrative functions in a smart contract, an attacker could, for example, create, destroy, or transfer tokens, pause functionality, manipulate data, and change or disrupt the way the smart contract operates.[86] One report notes that of the $1.4 billion stolen through code exploits in 2022, 90% occurred through "authentication issues, improper validation, and signature verification issues."[87]

Another exploit relates to a smart contract's inability to process data that is outside the range it is able to process (referred to as "integer overflow/underflow"), which may lead to unintended or unexpected outcomes. Smart contracts also are susceptible to "reentrancy attacks," which occur when an attacker can trigger a function on a particular smart contract repeatedly before the smart contract can finish executing the first triggering event of the function, creating a type of loop that allows for multiple executions of a command. This type of attack can result in an attacker withdrawing funds from a smart contract before the smart contract can update a ledger that tracks the allocation of those funds.

Governance-Related

Certain DeFi projects claim or aim to be governed by a community through, for example, the use of governance or voting tokens (see **ANNEX D**). Governance-related exploits aim to abuse the decision-making process (e.g., by amassing a majority of governance

[86] Private keys enable the signing of transactions in blockchain and DLT-based systems. These transactions can enable the transfer of crypto-assets, execution of smart contract functions or on-chain operations such as block proposals or approvals. Private key operational security is critical to prevent private keys from being stolen by malicious actors. While industry-standards for private key security best-practices are lacking, various methods for storing private keys exist, including, but not limited to, written on paper, stored in a local note application, stored on a hardware wallet or distributed by multi party computation (MPC). These methods commonly trade off security for ease of use and access. Bad actors use various schemes to steal private keys, including phishing and social engineering, to acquire access to machines or systems to extract the private keys of investors or DeFi protocol developers.

[87] TRM, *supra* note 22, at 32.

tokens/voting power) to implement changes or actions to the attacker's own benefit and against the general community interest (e.g., by requesting and executing a transfer of funds to the attacker's wallet). An attack on governance mechanisms can be facilitated through other types of attacks, e.g., by exploiting smart contract vulnerabilities, including through the use of a flash-loan attack.

Infrastructure-Related

Infrastructure components in DeFi are fundamental auxiliaries that can impact transaction processing, composability and other capabilities. Critical infrastructure components include oracles and bridges, which provide mechanisms for a multiplicity of data sources off-chain and cross-chain (from other DLT networks) to be utilized and relied upon to provide DeFi products and services in an originating DLT network (which is inherently siloed). Without the bi-directional movement of data between off-chain and cross-chain components, smart contracts that determine the parameters of a DeFi activity are limited to the data held on the originating DLT network. Attacks on these infrastructure components can occur from vulnerabilities that include low quality data collection and aggregation methodologies, reliance on a single point of failure, and the lack of an ability to dynamically reflect changes in reference data.

Tool: Flash Loans

Flash loans are used to borrow and repay crypto-assets in a single block recorded on a blockchain. They are a feature of DeFi that allow users to borrow assets with no collateral requirements, no credit checks, and no borrowing limits (except as based on the amount made available for borrowing by liquidity providers). This is possible because of *atomicity,* a feature of blockchains in which actions are either executed collectively in sequence in one block or fail collectively and absolutely. A flash loan is only valid within the transaction (within a block), which reverts to the pre-transaction state with no loss to the borrower (or lender) if they are unable to repay the loan within the same block.[88]

Flash loan attacks occur when an attacker borrows funds, uses them to effectuate a manipulative transaction, and repays the borrowed funds – all in one block. These attacks are popular because they require less upfront capital, provide large loan sizes, and are permissionless to execute. In addition, it is often difficult to identify malicious flash loan attackers due to the pseudonymity of blockchain addresses.

Flash loan exploits have been used to attack DeFi protocols in a number of ways. One involves an attack to exploit a smart contract vulnerability, permitting an attacker to drain funds from a smart contract. Another involves a "pump attack" that capitalizes on market inefficiencies and fragmentation. In DeFi markets, there is no industry agreed upon

[88] Arbitrage is a popular use case of flash loans as it allows traders to benefit from price differences across various exchanges. For instance, if token X is $10 on DEX A and $12 on DEX B, a user can use a flash loan to (1) borrow $10,000 worth of crypto-assets; (2) buy 1,000 token X for $10,000 at DEX A; (3) sell 1,000 token X for $12,000 at DEX B; and (4) pay back the $10,000 loan. However, this series of transactions must all occur in one block. In this scenario, the user will benefit by $2,000 minus fees. If, however, the user could not execute any one of the steps, or pay the fees, all of the steps in the transaction would fail.

centralized pricing source, and prices reported by centralized crypto-asset platforms may or may not be accurate, may be stale, or may not include pricing data from over-the-counter (OTC) markets. As a result, the same crypto-asset can be traded at different prices across different venues. In a pump attack, the attacker manipulates the relative price of two assets, for example, in a DEX liquidity pool and arbitrages away this price difference. Another flash loan related attack involves the manipulation of *oracles*. Oracles are infrastructure components that provide off-chain data, such as data from websites or APIs to on-chain smart contracts. Oracle manipulation in a flash loan context works similarly to a pump attack. In this case, the attacker may use funds from a flash loan to manipulate the price of a crypto-asset trading on a venue that is a reference for an oracle network (e.g., by adjusting the relative price of the two assets in the DEX-based liquidity pool or by conducting manipulative trades on a centralized crypto-asset trading platform) and the manipulated price is broadcasted across the oracle network to a DeFi protocol. The smart contracts using the manipulated price information cannot detect an anomaly and therefore continue to operate on the manipulated price information. The most high-profile oracle manipulations have often used flash loans; however, oracles may be manipulated through other means (e.g., flaws in the oracle's code). One blockchain analytics firm reported that more than 50% of the total amount stolen from attacks on DeFi protocols resulted from price manipulation techniques, such as those using oracle manipulation and flash loans.[89]

Tool: MEV Strategies

A developing area in DeFi involves what is known as MEV. MEV strategies encompass any strategy to capture or extract value from the ordering and inclusion of blockchain transactions, and can refer to value taken through arbitrage,[90] liquidation[91] and the payment of gas fees.[92] MEV strategies also refer to the exploitation of mempool data[93] that

[89] TRM, *supra* note 22, at 32.

[90] One type of MEV opportunity occurs through arbitrage. In the case that two crypto-asset platforms are trading a particular token at different prices, arbitragers can purchase the token on the platform with the lower price and sell it on the platform with the higher price. Some arbitragers use complex algorithms that identify profitable opportunities as quickly as possible. The concept of arbitrage is a profit-making strategy in traditional financial markets and is considered a part of efficient market dynamics.

[91] Another type of MEV opportunity occurs through liquidations of loans in DeFi lending/borrowing protocols that fall below their minimum collateral requirement. Typically, such protocols are over-collateralized, i.e., borrowers must post more collateral than they are borrowing. If the loan-to-value ratio exceeds the set limit, a market participant may close out the loan, taking the collateral. Participants can run specialized algorithms to monitor a network for transactions presenting liquidation opportunities and be the first to liquidate a loan. Liquidators can extract MEV from borrowers by liquidating a borrower's loan before the borrower can repay, then profit by selling the borrower's collateral.

[92] Another type of MEV opportunity is in the receipt of gas fees, or fees paid to miners/validators to process transactions.

[93] The mempool consists of transactions that are awaiting processing by the blockchain's miners/validators.

allows persons analyzing the mempool to maximize the profit they can make by the choice and sequencing of transactions to be proposed in a block to be appended to a blockchain. The most common exploitative strategies involving MEV occur when participants with visibility into pending transactions in the mempool can use that information to transact in a way that benefits themselves at the expense of the participants to the pending transaction. Variations of this strategy have been referred to as front running,"[94] "back-running"[95] and "sandwich attacks."[96] Such conduct in traditional markets would be classified as market manipulation.

While there is the potential for MEV strategies on various blockchains, the following descriptions are focused on MEV strategies relating to Ethereum (including through the use of applicable "MEV Boosting Software"). The key players currently are:

- **Developers:** establish a protocol, creating potential for MEV opportunities, or create software tools, such as MEV Boosting Software, to extract MEV.
- **Validators:** determine which transactions pending in a mempool to include in blocks and in what order. Typically, a validator will decide to order the block with the highest gas fee paid at the front and order in this way until the block is complete.
- **Searchers:** seek to identify and capture MEV opportunities, often through the use of complex algorithms called *bots*. Typically, searchers will pay higher gas prices to place their transactions at specific positions within a block. Some validators could have agreements with searchers to effectuate the searcher's MEV strategies in exchange for a portion of the MEV captured.

[94] Front-running occurs when a participant observes a pending transaction that is likely to impact the market in a particular way. The participant will propose a transaction based on that information and attempt to have it execute prior to the pending transaction. A miner/validator could execute this attack through re-ordering of transactions on a proposed block; a searcher might attempt to pay a higher gas fee or collude with a miner/validator to move the transaction ahead of the pending transaction. One study calculates losses due to frontrunning attacks between May 2020 and April 2021 to have amounted to more than $100 million USD. *See* Agostino Capponi et al., *Inefficiencies in Public Distributed Ledgers* (Dec. 31, 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3997796.

[95] Back-running occurs when a participant orders their transaction to be executed immediately after a pending transaction. This type of attack might be profitable, for example, if the pending transaction is to create a new pair for trading on an automated market maker (AMM). An attacker can employ back-running bots to monitor the mempool for new token pair listings or liquidity pools created on decentralized exchanges. When a bot finds a new token pair listing, it can place a transaction order immediately after the initial liquidity and buy as many tokens as possible, leaving only a small amount for other traders to buy later. The bot can then wait for the price to go up after other traders have purchased the tokens and sell at a higher price for a profit.

[96] A sandwich attack occurs when a participant places two transactions, one before and another right after a pending transaction. Searchers typically use sandwich attacks to extract MEV from unsuspecting traders on decentralized exchanges by manipulating the price of an asset. For example, a trader can identify a token a victim is about to buy and make a trade to push the price up, then sell the token immediately after the victim's buy order has further increased the price.

- **Block Builders:** construct blocks from proposed transactions. This is done by running algorithms and simulations to order the bundles of transactions in a block template that maximizes profit. Builders then bid for and buy the validators' blockspace, facilitated by one or more relays, so their execution payloads are proposed to the blockchain.
- **Relays:** facilitate communication interfaces that aggregate blocks from builders to provide the most profitable block to proposers for validation.
- **Proposers:** a validator that has been randomly selected amongst all the validators to build a block for a given slot. Proposers may pay block builders if their proposed block is appended to the blockchain.
- **Impacted Users**: engage in transactions on a blockchain whose execution is affected by MEV strategies.
- **MEV Boosting Software**: seeks to maximize MEV opportunities for miners/validators.

MEV strategies are evolving, and more skilled participants, or those who collude with others, may be gaining more income from MEV strategies. This dynamic may lead to increasing concentration effects as those participants can gain more control over the network. The switch from Ethereum PoW to PoS[97] resulted in changes to the MEV space including, but not limited to, a terminology change from "Miner Extractable Value" to "Maximal Extractable Value," an increase in MEV rewards in proportion to block rewards, and a change to the entities in the MEV supply chain (such as validators taking the place of miners). This switch may lead to centralizing effects in Ethereum PoS due to reduced constraints on hardware requirements and natural pooling of ETH at entities such as centralized trading platforms who dedicate resources to sophisticated MEV strategies and create economies of scale.

As Ethereum blocks are built from transactions, parties who seek to obtain MEV will compete for transactions. These participants can access transactions to locate MEV opportunities in two primary ways – through searching transactions on the blockchain/mempool or through access to exclusive transaction order flow. As users want their transactions to be included in a block, there is the potential for users to submit their transactions through a limited number of operationally sophisticated entities, and

[97] Proof of Work (PoW) commonly refers to a blockchain consensus mechanism where miners compete to solve cryptographic puzzles in order to earn the ability to add new blocks to the blockchain and receive a reward of newly-minted crypto-assets.
See, e.g., https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/. Proof of Stake (PoS) commonly refers to a blockchain consensus mechanism where validators stake crypto-assets to earn the ability to add new blocks to the blockchain and receive a reward of newly-minted crypto-assets. A validator's stake can be reduced (or 'slashed') through behavior harmful to a blockchain. *See* https://ethereum.org/en/developers/docs/consensus-mechanisms/pos.

validators with a high inclusion rate of transactions are more likely to obtain transaction order flow.

Dominant validators with sophisticated resources to develop MEV strategies are potentially able to propose the most blocks on the network and extract the most MEV, providing outsized rewards compared to validators with less sophisticated or no MEV strategies. This could enable validators providing staking as a service (SaaS) to offer higher returns to customers, potentially attracting more customers to deploy more validator nodes and increase dominance on and centralization of the network. Solo-staking validators could also earn more rewards from the addition of sophisticated MEV strategies to their validation operations. In both hypothetical examples, sophisticated MEV strategies could result in more rewards earned that can then be staked to control more validators on the network thus potentially increasing centralization risk.

These dynamics could lead to market concentration and, as is the case with other concentrated markets, could give a limited number of entities the potential to extract higher profits from users and to behave in other non-competitive manners such as collusion or censorship of certain transactions.

To address this potential centralization issue, core developers in the Ethereum 2.0 network reportedly have proposed a “proposer-builder separation” (PBS), such that a separate group of participants called “block builders” will build a block of transactions and a separate group of participants will accept the block without knowing the contents of any block until after it is selected. With PBS, block builders presumably would accept transactions from users and searchers, entities who submit groups (“bundles”) of transactions in a specific order to builders and compete to build the most profitable blocks possible from those transactions. Block builders would then send blocks through intermediaries known as relayers to block proposers who would simply pick the highest-bid blocks proposed by block builders and validate the blocks. However, this is merely a proposal and any implementation of PBS into the Ethereum core protocol will likely take time.

As MEV can be extracted based on ordering of transactions in a block, current attempts to minimize MEV opportunities center around increasing opacity in the transaction order, either through anonymizing transactions, through batch auction, private mempools and other market structure changes. There have been reported efforts to “democratize” MEV operations though open-source software to lower the entry to MEV operations and apply the PBS concept outside of the core Ethereum protocol.

ANNEX C – DATA GAPS AND CHALLENGES

Accurate and complete data is critical to the understanding of any financial ecosystem. Specifically, regulators rely on data to monitor a financial ecosystem and its participants, to flag abnormalities and trends, and to investigate non-compliance and illegal activity.

The data needs of regulators and supervisors span many dimensions of the DeFi ecosystem. These dimensions include:

- *Transaction-level data*: Transaction-level data between and among all participants, including smart contracts.
- *Protocol-level data*: Smart contract addresses and underlying code, as well as URLs and programming of user interfaces.
- *Participant data*: Data concerning key participants, including software developers, large investors (e.g., whales, VCs, institutional investors, etc.), and governance/voting token holders.[98]
- *Oracles and other DeFi Infrastructure*: The function, inputs and vulnerabilities of infrastructure, including layer 1 blockchains, layer 2 networks, oracles, bridges, etc.

Available data

As highlighted in the 2022 Report and in this report, the provision of DeFi products and services typically involves on-chain and off-chain activities. Therefore, data relevant to DeFi are located on-chain and off-chain, as well. To the extent data is on-chain, it requires tools and expertise to interpret and may not be in human-readable format. To the extent data is off-chain, it could be inaccessible. Even if off-chain data is made available through, for example, a website or API, the data likely is not audited or otherwise verified, and may be unreliable.

Two key metrics derived from on-chain data are commonly associated with DeFi:

- **Aggregate flow statistics**, which allow analysts to gauge the interest market participants may have in a protocol. Flow data can be aggregated either within one blockchain to determine the preeminence of a protocol within a given blockchain, or across all blockchains in order to determine the protocol's importance in the overall DeFi ecosystem. Flow statistics can be derived by looking at changes in values that are originally derived from a blockchain's publicly available data. Alternatively, some protocols contribute statistics and data to various aggregators and/or dashboards.
- **Total Value Locked** (TVL), reportedly representing the accumulated deposits by protocol users.

[98] Specific data on institutional investor participation could improve the measurement and understanding of the interconnection risks.

However, these metrics, though commonly used, lack standardisation and should be scrutinized in terms of the information they convey. In the case of TVL for example, certain types of protocols (e.g., liquidity pools, bridges, etc.) use *locked value* to mint new derivative, synthetic or *wrapped* tokens, which can themselves be deposited in other DeFi applications. This feature of DeFi has sometimes been referred to as re-hypothecation and may result in a crypto-asset and its derivative, synthetic, or wrapped version being counted multiple times for TVL purposes (often called *double-counting*.)[99] It is also important to note that TVL values fluctuate with the underlying market values of the crypto-assets on which they are based. Aggregate flow data tends to be based on TVL data (e.g., changes in TVL for a given protocol), so this data has similar shortcomings as TVL data. In addition, protocol-contributed data, such as TVL, can be inaccurate for other reasons, and it is not always validated against blockchain activity.

A recent BIS report noted three types of metrics that authorities can monitor to assess risks in DeFi: (1) indicators that gauge the overall size and evolution of the sector; (2) indicators designed to assess financial vulnerabilities; and (3) indicators that gauge the potential for spillovers by tracking and assessing interconnections between DeFi, Centralized Finance (CeFi), traditional finance and the real economy.[100]

Some metrics that may be useful for analyzing any particular DeFi protocol are:

- TVL
- aggregate flow
- market value of a protocol (measured by the number of outstanding tokens multiplied by the market value of the token -- sometimes referred to as “market capitalization”)
- number of users
- governance structure and operation
- linkages with other entities (i.e., blockchains, bridges, oracles, etc.)
- multi-sig thresholds for changing smart contracts
- numbers of pairs traded, number of trades, liquidity flows in/out, market share by volume (for DEXs)
- lend/borrow amounts and rates, repayments, liquidations, deposits and withdrawals, liquidation thresholds (for lending/borrowing protocols)
- offered yields (for aggregators or liquid staking providers)
- hacks/operational issues

[99] Certain TVL data providers claim to be able to identify funds that are used multiple times and offer “clean” TVL metrics.

[100] BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 17-18 (July 2023), https://www.bis.org/publ/othp72.pdf.

- links to addresses known to have received funds from or used funds for illicit activities
- total value of crypto-assets received from illicit addresses
- links to fraud reports
- VC and other early investors

Some metrics that may be useful for analyzing any particular blockchain are:

- TVL
- aggregate flow
- governance structure and operation
- number of validators or miner nodes
- number of unique addresses on a blockchain
- number of active addresses on a blockchain
- number of transactions
- number and types of smart contracts/protocols
- hacks/operational issues
- links to fraud reports
- developer activity/growth
- gas prices/transaction fees
- MEV opportunities and dynamics
- VC and other early investors

Some metrics that may be useful for analyzing the DeFi market more broadly are:

- Retail investor participation
- TVL per protocol type (i.e., DEX, lending/borrowing, aggregator)
- aggregate flow per protocol type (i.e., DEX, lending/borrowing, aggregator)
- interest in crypto-assets over time based on web searches (media coverage)
- Demographic/geographic ownership of crypto-assets
- Market concentration (e.g., using Herfindahl-Hirschman Index[101])
- Interest rates offered in DeFi
- Market prices and volatility
- Open crypto-asset derivative positions, long and short

[101] Herfindahl-Hirschman Index (HHI) is a measure of market concentration. It can be used to determine the relative concentration of market share in a given market. *See* U.S. DEPT OF JUST., HERFINDAHL-HIRSCHMAN INDEX, https://www.justice.gov/atr/herfindahl-hirschman-index.

- Stablecoin metrics
- Interconnectedness, through metrics on blockchains, protocols, oracles, bridges, etc.
- VC and other early investors

When using any of the metrics above, it is important to keep in mind that the metric may be based on industry reported, unverified data; nevertheless, the metric may be useful in a relative sense or for monitoring purposes, absent the availability of verifiable data sources. Metrics such as these, for example, can be used to rank activities in terms of their usership and growth and can help regulators begin to construct a picture of what is happening in DeFi. This information could help regulators decide how to allocate resources for potential regulatory action.

Data Gaps

Despite that there are DeFi data providers and analytical tools, some of which are open source, there are significant data elements that are not publicly available. The inaccessibility of relevant data increases the challenges to market surveillance and reduces the ability to monitor activity. For example, ownership concentrations of governance tokens may only be partially visible on-chain, as significant amounts may be held by a centralized crypto-asset platform in an omnibus wallet address. In addition, communication and coordination for project governance often takes place on social media, and typically only individuals granted access to the relevant chat groups can observe relevant discussions. The financial resources of a DAO or DeFi protocol can be opaque, for example, part of the resources could appear on-chain, and part could be held off-chain. Fund transfers relating to DeFi activity can take place on private networks. These transfers can occur between DeFi and other crypto-asset market participants and can involve both fiat currencies as well as crypto-assets for the transfer of value. Increasing the ability of regulators to decipher on-chain data and to have access to off-chain data can provide for a more holistic view of a DeFi arrangement or activity, including its interconnectedness with other market participants and activities.

- **Lack of Financial Reporting**: DeFi protocols typically do not publish formal or informal financial data, nor do they typically engage auditors to opine on their operations or internal controls.
- **Lack of Broad Market Data**: DeFi does not have a self-regulatory organization that collects, compiles and disseminates data across protocol types.
- **Failure to Register/License:** Because DeFi protocols generally have not registered or licensed as exchanges, brokers, dealers, hedge funds, swap dealers, asset managers, or other regulated entities, the protocols may be in non-compliance with requirements that would facilitate regulators' ongoing oversight activities that include understanding and scoping the entirety of a protocol's operations. Jurisdictions maintain data sets for entities subject to regulation for particular activities.

Data Providers

Data providers for crypto-asset related data are highly specialized, fragmented in what they offer, and can be expensive. Providers tend to cover different data sets and analyze different aspects of the data. For example, some cover various blockchains and/or crypto-assets. Some focus on transaction analysis on particular blockchains and provide, for example, risk-scoring of entities for AML purposes. Others focus on smart contracts and potential vulnerability analysis. Still others offer more traditional financial data and research, such as pricing, research, and market trends. In addition to vendors, DeFi data can also be accessed through a variety of online interfaces. Use of these tools can require specialized training and significant resources and cost. Accordingly, it may be difficult and costly to arrange comprehensive coverage across the entire DeFi market. It is also important to assess where a particular vendor sources its data to evaluate whether there are risks that the underlying data is incomplete or inaccurate. The following table identifies some, but not all, data needs and potential gaps/challenges for illustrative purposes.

Table: Data Needs and Gaps

Layer	Potential Use Cases for Regulators	Data Needs	Data Availability	Potential Gaps/Challenges
Settlement Layer (including blockchains and Layer 2 solutions)	Assessing compliance with applicable laws and regulations; analyzing consensus mechanisms and activities; analyzing transactions and transactional dynamics; analyzing MEV activities	Blockchain transactional data; mempool data	On-chain data; node peers, client distribution, IP addresses; mempool data; MEV data; online blockchain explorers and other data analytics providers	On-chain data is voluminous, can be difficult to interpret, and requires specialized skills and significant infrastructure costs; mempool data may not be available, is unique to individual nodes, and complex to analyze; transactional information is pseudonymous and can be anonymity enhanced
Asset layer (including tokens)	Assessing compliance with applicable laws and regulations; Analyzing token creation, issuance, distribution,	See above; smart contract code concerning tokens	See above; GitHub/GitLab (central repositories for code underlying many smart contracts); market data from DeFi	See above; there is no assurance that the information available on GitHub/GitLab or through blockchain explorers reflects what occurs on-chain; source code is not always publicly

	and functionality; monitoring fund flows, including proceeds of illicit activity		protocols and off-chain centralized crypto asset platforms; social media and other off-chain sources	available; Market data is not always audited, data standards and aggregation methods are fragmented and lacking
Smart contract layer (including DeFi protocols, DAOs and bridges)	Assessing compliance with applicable laws and regulations; assessing functionality, governance, and vulnerabilities; monitoring systemic importance and interlinkages	See above; smart contract code and other data concerning DeFi protocols	See above; smart contract analysis and assessment tools; governance voting websites; Market data for DeFi protocols, DAOs and bridges assets under management	See above; reading and analysing smart contracts requires a specialized skillset
Application Layer (including user interfaces, websites, aggregators)	Assessing compliance with applicable laws and regulations; monitoring sector developments and growth	See above; website, web extension, or mobile/desktop application of a given user interface or aggregator; information on parties maintaining the user interface or aggregator; code for optimisation, trading and other algorithms	See above; disclosures; VPN blockers; user traffic; integrations with other platforms	See above; the underlying on-chain smart contracts and functionality could be obfuscated

ANNEX D – DEFI GOVERNANCE

Broadly, governance refers to the actions and processes managing the control and direction of an entity. Governance encompasses a number of elements, including the allocation of authority, both legal and operational; the ways that authority can be, and is, exercised; and the broader set of practices, policies and procedures by which an entity is organized and administered. An entity's governance structure dictates the mechanism through which decisions are made, directions are given, and ultimately, how control and influence are exercised within the entity.

Blockchain "Layer 1" Governance

Governance of the settlement layer (layer 1) of a typical blockchain typically occurs both on-chain and off-chain. For major blockchains today, core developers usually put forth a proposal for debate, largely through an informal process using off-chain social media-based communications among core stakeholders, including protocol developers, node operators and validators. Core developers may consider input from other stakeholders and the proposal may evolve until the core developers propose a final implementation. At that point, adoption of a change to the core protocol of a blockchain will depend upon a majority of validators choosing which version of the core protocol they will run.[102]

This process suggests several observations. First, it is the developers who must code any agreed proposal for it to be implemented. Thus, protocol developers may have outsized influence relative to other stakeholders in the final form any such proposal takes. It is also the case that users and other stakeholders may have limited access to all the information regarding a proposal including its underlying code. Also, whether and to what extent the final outcome is adopted is decided ultimately by the network validators, who determine which version of a layer 1 core protocol to participate in. To the extent that there is disagreement about adoption of a core protocol change, a hard fork may result in a split of participants continuing to transact on two separate networks. Control of validator nodes can be significantly concentrated in major blockchains. This may result in de facto control of a layer 1 blockchain by a small group, i.e., core developers and validators.

Decentralization is a term that can describe various aspects of a DeFi arrangement or activity, such as ownership of an enterprise providing a product or service, voting power over the enterprise or any aspect of it, control of user or investor assets, network design of an underlying blockchain (settlement layer), or off-chain infrastructure such as web servers that provide application components, among others. There is no agreed definition (even among industry participants) of what causes an arrangement or activity to be considered

[102] *See* ETHEREUM, INTRODUCTION TO ETHEREUM GOVERNANCE, https://ethereum.org/en/governance/ (providing a summary of how governance for the Ethereum network works, including key stakeholders, process steps, and features).

decentralized, such that there is no concentration of ownership, voting power, or control as to the product or service, enterprise or user assets. While those who offer DeFi products or services may claim to be decentralized, most DeFi arrangements may in reality have a significant level of centralization. For example, founders or other participants may retain control or significant influence over aspects of an arrangement or activity. 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 they may continue to be controlled by centralized parties. In some cases, those aspects that are up for vote are not ones that relate to the operation of a project at the enterprise level. Most DeFi arrangements and activities today rely on centralization in one or more areas and are decentralized in name only.

It is worth positing that DeFi products and services are a result of the person(s) and entit(ies) that create, offer and maintain them. These persons and entities typically determine from a project's inception how participants are or can be organized, including whether participants will or can organize as a *DAO,* a foundation, or something else. They also often design ways for participants to influence how certain aspects of a project's protocol will operate in the future, including by giving certain participants the ability to alter smart contracts or other aspects of the project's protocol. These ways can include the use of administrative keys,[103] multi-sig and time-lock mechanisms,[104] code updates, and voting tokens (often referred to as governance tokens). These entities and individuals in most cases establish the fundamental features of the protocol, such as how decisions will be made, who makes those decisions and for what aspects of the project, and who has access to information concerning those decisions. This section explores how novel organizational structures (DAOs) and governance structures (governance/voting tokens) can be analysed for the purpose of determining control or influence.[105]

The 2022 Report noted that some DeFi market participants claim that governance is decentralized. DeFi projects may use various mechanisms to distribute governance roles, such as DAOs and governance/voting tokens, in order to provide evidence of decentralization. However, there are many different permutations of governance arrangements and the role they play within an enterprise. The fact that elements of a DeFi

[103] Administrative keys refer to cryptographic key information that permits a holder of that key information to make certain changes to a smart contract including, potentially, by permanently disabling the smart contract. Administrative keys effectively can place ultimate control over a smart contract in the hands of the administrative key holder(s).

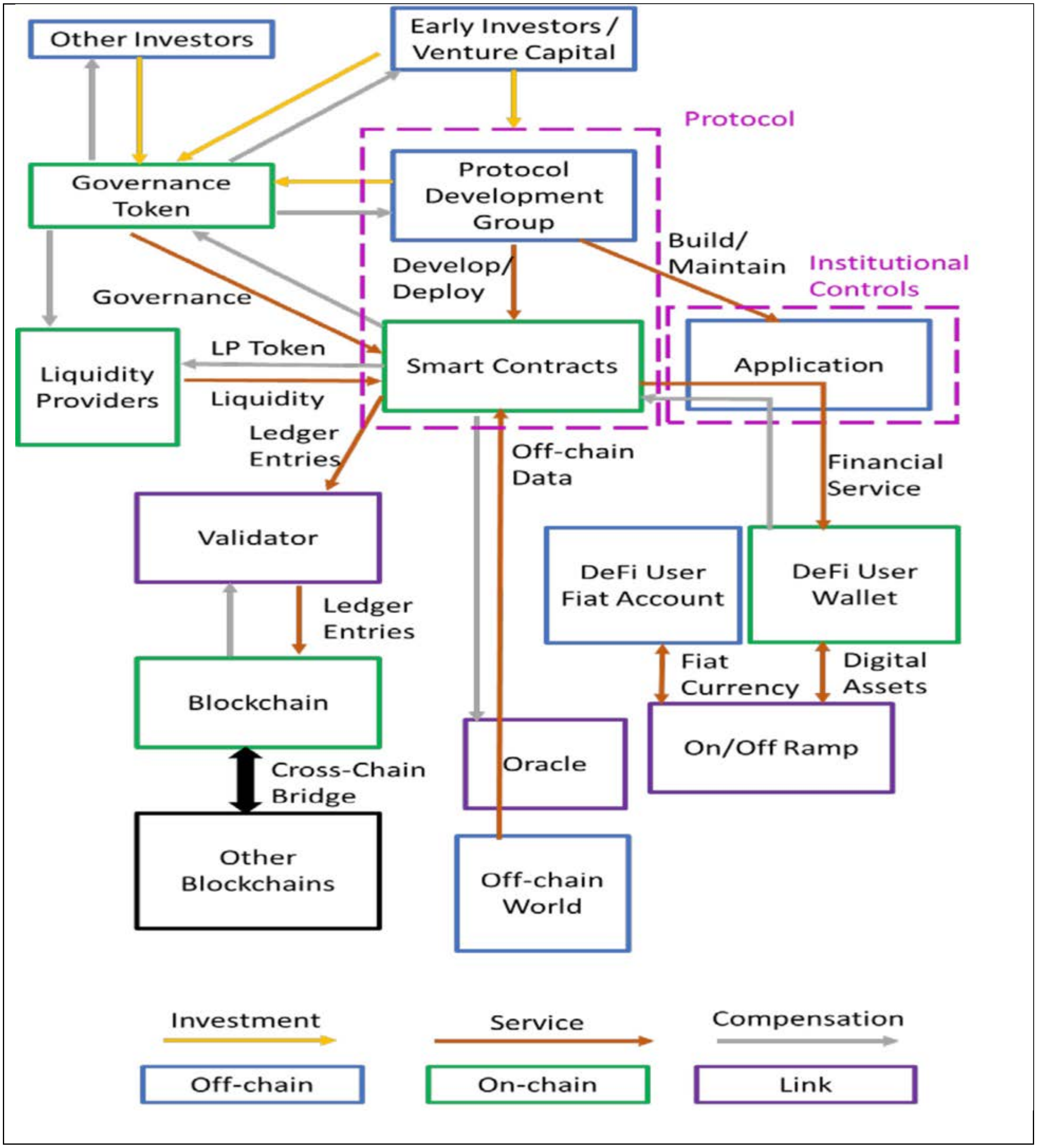
[104] Multi-signature ("multi-sig") refers to smart contracts that require a number of holders of cryptographic key information to agree on an action before it takes place, indicating that agreement through using the key information to "sign" a transaction. Some multi-sig mechanisms require unanimous agreement, while others require a given number of a set of participants to agree to the action. Time-lock smart contracts implement delays in executing a function until a given amount of time has passed. Such delays can allow for additional governance activities (such as deliberations) before the action considered in a time-lock contract is performed.

[105] A DAO can, but need not, employ governance or voting tokens. Conversely, a project that uses governance or voting tokens need not be a DAO.

arrangement or activity may be viewed as distributed or subject to community vote does not mean that the arrangement or activity itself is decentralized. As discussed below, governance/voting tokens currently may play a limited role in 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. Furthermore, while DAOs are presented as a solution to community governance, DAOs and their development are still in the nascent stages. Additionally, while a particular DeFi protocol may aim to be resistant to censorship or collusive control, there may still be an ongoing dependency of protocol development and functionality on central actors, such as developers or founders. In DeFi, the issue of governance must be evaluated from both the smart contract or protocol level as well as at the enterprise level. Examining DeFi project's governance structure will typically reveal potential regulatory touchpoints.

Enterprise Level - The Big Picture

The 2022 Report noted that the provision of DeFi products and services relies on the contributions of various stakeholders, each of whom has an important role to play and expects to earn a profit through participation. These stakeholders include the developers and promoters of a DeFi project, investors in the project, users, service providers, and blockchain networks. The 2022 Report includes a detailed discussion of the *Big Picture* to assist in analyzing DeFi arrangements and activities at the enterprise level. In particular, persons and entities develop and deploy the software and other components through which DeFi operates. These persons and entities often obtain funding for their development efforts from investors in traditional capital raising and via crypto-asset offerings. As protocols are developed, these persons and entities often create a reserve or treasury to hold fiat currencies or crypto-assets for purposes of funding future refinements and development of the protocol. These persons and entities may either control these reserves themselves or may create a different organization to manage the reserve or treasury. The specific organizational forms that develop and deploy protocols and those that are responsible for ongoing activities can vary. Common types include traditional corporate entities, foundations that often hire others to work on the protocol, and DAOs. DAOs are becoming increasingly an organizational choice for DeFi projects. Whatever organizational form a particular DeFi project takes, and whatever tools it may use to carry out its operations, it is important to focus on the DeFi arrangement or activity at an enterprise level. Often, this viewpoint will reveal who has control or sufficient influence over the operations of the enterprise so as to be responsible for its activities. Below is a reproduction of the Big Picture from the 2022 Report, which contains a detailed explanation and breakdown of each component of the Big Picture: capital formation, development and deployment; use and investment; and settlement.



Decentralized Autonomous Organizations (DAOs)

As the 2022 Report explained, some DeFi market participants experiment with new organizational structures in an attempt to achieve more decentralized systems. A DAO is a relatively new type of organizational structure that purportedly focuses on community, as compared to centralized, governance. There is no agreed definition of what constitutes a DAO, even within the industry. DAOs and their structures are evolving. According to one industry source, as of August 2023, there are more than 25,000 DAOs controlling treasuries worth $22.5B.[106]

In brief, a DAO typically is a form of coordination for a group of people who coalesce around common goals. DAOs vary in structure and complexity. They can use smart contracts and other technologies to facilitate a number of processes, such as communicating, coordinating, and incentivizing individuals to act collaboratively.

DAOs may have different legal characterizations depending on the particular jurisdiction. In some jurisdictions, a DAO may be recognized as a unique and separate type of legal entity. In others, DAOs may be analyzed under frameworks that already exist for partnerships, joint ventures, associations, limited liability entities, or similar structures.[107] The legal organizational treatment for any particular DAO will depend on the facts and circumstances, including how it is structured, and the applicable law within a jurisdiction in which the DAO has a presence for purposes of any particular authorities' remit. However, to enable the principle of "same activity, same risk, same regulatory outcome," regardless of the legal characterization of a DAO from an organizational standpoint, the focus from a regulatory and supervisory standpoint typically will be on the activity the DAO is engaging in, such as whether the DAO's activities or structure involves a financial instrument, including a security, or related activities, in a particular jurisdiction.

Why are DAOs Claimed to be Decentralized?

DAOs are, at their essence, organizations of humans. DAOs are described as "decentralized" because they may claim that they operate without reliance on centralized management. DAOs are described as *autonomous* because they claim (or aim) to operate in an automated manner in accordance with the rules encoded in self-executing code (smart contracts) rather than in accordance with traditional articles of association or shareholders agreements.[108]

The common perception may be that in DAOs, entity level decisions such as what action the DAO takes or changes or alterations to the operation or activities of the DAO are determined by its membership, and are not dependent on, determined by, or controlled by any person or group of persons. In practice, however, the extent of actual voting

[106] https://deepdao.io/organizations.

[107] *See, e.g.,* CFTC v. OokiDAO, Case No. 3:22-cv-05416 (N.D. Ca. June 8, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23 (entering a default judgment order against a DAO whom CFTC charged with operating an illegal trading platform and unlawfully acting as a futures commission merchant); Sarcuni v. bZx DAO, Case No. 22-cv-618-LAB-DEB (S.D. Ca. Mar. 27, 2023), https://casetext.com/case/sarcuni-v-bzx-dao (finding that plaintiffs stated facts sufficient to allege that a general partnership existed among token holders of a DAO).

[108] Often, token holders will have some ability to participate in certain decisions, such as aspects of a project's protocol, electing working group contributor or leaders for the DAO, or administering the DAO's treasury. Often, in practice, a DAO's creators, or others, will still exercise control or sufficient influence, whether through a concentration of voting power, administrative or other gatekeeping functions, or otherwise.

participation can be low[109] and a DAO's *governance* actions through voting tokens can have a very concentrated distribution, with less than 1% of token holders controlling 90% of voting power of DAOs.[110] Moreover, the types of decisions that can be voted on can be quite limited.

Whether and to what extent any particular DAO actually is decentralized or autonomous depends on the facts and circumstances and requires an in-depth examination of how that DAO is structured and how it is operating in reality.

Regulatory Actions Involving DAOs

The DAO Report

In 2016, a project called The DAO launched on the Ethereum blockchain, raising $150 million in ether from investors in exchange for crypto-assets called DAO tokens, which entitled holders to vote on blockchain-based projects that would receive funding from The DAO. The DAO's plan was to invest funds in such projects, with profits flowing back to DAO token holders. Before the DAO had commenced funding projects, an attacker exploited a bug in the DAO's smart contract code and was able to divert about one-third of the funds held in the DAO's treasury. A period of uncertainty followed, with the members' remaining funds essentially immobilized within the DAO. Ultimately, and controversially, the effects of the attack were reversed (and the funds returned to investors) through a process known as forking, in which the blockchain was essentially split into two separate chains (Ethereum and Ethereum Classic). On the Ethereum chain, DAO funds could be reclaimed by investors. On July 17, 2017, the US Securities and Exchange Commission (SEC) issued a *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Exchange Act Rel. No. 81207) (the DAO Report), explaining the application of US federal securities laws to The DAO. The DAO Report explained that The DAO tokens had been offered and sold as investment contracts, and therefore securities, and that the offering should have been registered under the federal securities laws since no exemption to registration applied. The DAO Report also made clear that the US federal securities laws may apply to various activities without regard to the form of the organization or technology used.[111]

[109] Youssef Faqir-Rhazoui, Javier Arroyo & Samer Hassan, *A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain*, 9 J. INTERNET SERV. & APPL. 12 (2021), https://jisajournal.springeropen.com/articles/10.1186/s13174-021-00139-6.

[110] *Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated*, CHAINANALYSIS (June 27, 2022), https://blog.chainalysis.com/reports/web3-daos-2022/.

[111] *See* Release No. 81207, U.S. Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

The Ooki DAO

On September 22, 2022, the US Commodity Futures Trading Commission (CFTC) filed an enforcement action in district court against a DAO called the Ooki DAO, alleging that the Ooki DAO was "illegally offering levered and margined retail commodity transactions in digital assets; engaging in activities only registered futures commission merchants (FCM) can perform; and failing to adopt a customer identification program as part of a Bank Secrecy Act compliance program, as required of FCMs."[112] The district court permitted the CFTC to achieve service of the Complaint by alternative means, consisting of providing a copy of the summons and complaint through the Ooki DAO's "Help Chat Box," and an online discussion forum on the Ooki DAO's public website.[113] On June 8, 2023, the district court judge entered a default judgment order that requires the Ooki DAO to pay a civil monetary penalty; orders permanent trading and registration bans; and orders the Ooki DAO, as well as any person or entity acting on its behalf providing web-hosting or domain-name registration services in the US, to shut down the Ooki DAO's website and remove its content from the Internet. The Court held that the Ooki DAO is a person for purposes of the Commodity Exchange Act and thus can be held liable for violations of the law.[114]

Different Types of DAOs and their Uses[115]

Like other organizations, DAOs are heterogeneous, and their goals, scale, and participants can vary widely. DAOs can be organized for various stated purposes, whether charitable, profitable, social or technological. Although most DAOs have been focused on online-

[112] *See* CFTC v. Ooki DAO, Civ. No. 3:22-cv-5416 (N.D. Ca. Sept. 22, 2022), https://www.cftc.gov/PressRoom/PressReleases/8590-22.

[113] *See* CFTC v. Ooki DAO, Civ. No. 3:22-cv-05416-WHO (N.D. Ca. Dec. 20, 2022), https://storage.courtlistener.com/recap/gov.uscourts.cand.400807/gov.uscourts.cand.400807.63.0.pdf

(holding that service has been achieved).

[114] *See* Release No. 8715-23, Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory (June 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23.

[115] Bud Hennekes, *The 8 Most Important Types of DAOs You Need to Know*, ALCHEMY (April 6, 2022), https://www.alchemy.com/blog/types-of-daos; Georgia Weston, *Know The Different Types Of DAOs*, 101 BLOCKCHAINS (April 29, 2022), https://101blockchains.com/types-of-dao/; *Full 2022 Guide to Different Types of DAOs*, MORALIS WEB3 TECHNOLOGY (2022), https://moralis.io/full-2022-guide-to-different-types-of-daos/.

related projects, their presence has been expanding.[116] DAOs can be grouped into a number of general categories, each purportedly designed to serve a specific purpose.[117]

DAO Participants

The following participants are generally involved in a DAO:

- **Developers and Founders:** Developers and/or founders typically create, code, promote and deploy a DAO, including its associated smart contracts. Typically, they establish the structure through which governance will be effectuated.
- **Members**: Some DAOs are set up so that membership is based on the ownership of tokens, often called DAO tokens or governance tokens. These typically provide certain types of voting rights, which may or may not relate to the operation of the DAO or its activities. Others establish their membership in other ways.
- **Employees/Contractors**: DAOs can hire individuals or entities for a wide range of roles, including for accounting and legal services. Whether or not a DAO has a manager or a managing group responsible for hiring and other managerial or administrative duties will depend on the particular DAO.
- **Working Groups:** Many DAOs have adopted a division of labor into working groups (also known as workstreams or subDAOs), each of which may comprise a group of members or other contributers to the DAO. As compensation for serving on such a working group, a contributer typically is paid by the DAO from its treasury. Working groups have focused on such topics as product development, operations, growth and marketing. These groups might manage things like

[116] Amir Ghavi et al., *A Primer on DAOs*, THE HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE (Sept. 17, 2022), https://corpgov.law.harvard.edu/2022/09/17/a-primer-on-daos/.

[117] Industry reports describe various types of DAOs, including the following: **protocol DAOs** (facilitate operational choices about certain aspects of a DeFi protocol, such as a DEX or borrowing/lending protocol); **grant DAOs** (facilitate funding of projects, typically associated with a DeFi protocol or ecosystem; typically are established by the protocol developers or close affiliate; typically disburse treasury funds to support projects to develop a protocol or ecosystem); **philanthropy DAOs** (support socially responsible initiatives); **social DAOs** (bring together individuals to create communities and working groups around social issues; often form exclusive memberships to organize social events or to provide some other social benefit to members); **collector DAOs** (pool funds to purchase something, often a digital good, such as a 'blue chip' NFT or other digital collectible; each member typically owns a pro rata share of the item purchased, corresponding to their pool input); **investment and venture DAOs** (pool capital to invest, typically in DeFi start-ups and protocols; aim to provide access to investment portfolios that may not be available in traditional finance); **media DAOs (**create media platforms, often aiming to create platforms where content creation is driven by the community and individuals in the network are incentivized to contribute based on the ability to earn profits from participation; **subDAOs** (manage specific functions such as operations or partnerships within the DAO); **employment DAOs** (facilitate matching of human skills with demand; contracts members' skills to other individuals and entities).

upgrades to a protocol, grants programs to incentivize protocol usage, and promotional campaigns, respectively. In addition, DAO collectives have formed to fund and support development.[118] These types of organized management are a part of the facts and circumstances analysis when evaluating the treatment of DAOs under applicable regulatory frameworks.

Third-Party Service Providers: DAOs often hire third parties to provide legal, recordkeeping, accounting, banking or other services. There are different mechanisms a DAO may use to engage these entities, many of which may entail human involvement in selection and retention of these third parties. A DAO could authorise, through a governance vote or otherwise, the use of third-party service for a particular purpose. The DAO could also authorize an individual or a group to create and capitalise a traditional corporate entity for the purpose, for example, of entering into a corporate agreement on behalf of the DAO or delegating a scope of decision-making to a particular individual or group. DAOs also use third-party service providers to host forums for discussion and voting, as well as to store code, create open-source projects and build software. Some third-party service providers offer a combination of these services. Third party services are also used to enforce *token-gating* where access to certain information is restricted based on ownership of a token, particularly the DAO's token. The extent to which these DAO activities are initiated or controlled by a person or group of persons is a facts and circumstances determination.

<u>DAO Formation</u>

DAOs are created by persons or entities who typically will sell crypto-assets or otherwise raise capital to further the DAO's stated purpose. The DAO typically will issue crypto-assets in accordance with a plan of distribution put in place by the persons or entities.[119] Often the creators of a DAO will deposit the DAO's assets into its treasury and assert that the management of the DAO will take place through the votes of token holders. Treasuries are generally used to fund the DAO's initiatives, and typically comprise tokens from an initial distribution and fees charged to users by a protocol for its use.

[118] *See, e.g., 5. Pilot: May '22 - May '23*, PROTOCOL-GUILD, https://protocol-guild.readthedocs.io/en/latest/5-initial-pilot.html.

[119] DAO members typically become members by purchasing or otherwise obtaining crypto-assets issued by the DAO (DAO tokens) although, depending on design, some members need not hold tokens. DAO tokens typically can be purchased by anyone interested in joining a DAO, in exchange for other crypto-assets or for some form of contribution or service to the DAO. DAOs distribute DAO tokens in many of the same ways other crypto-asset token issuers distribute them, i.e., through direct distribution to purchasers or users, through initial purchasers who then on-sell them to a broader set of purchasers (akin to underwriting), or through platforms or protocols (who, themselves, could be akin to issuers, brokers or dealers). They may also distribute them through "air drops," often to founders, members who provide services to the DAO, members who have been most actively involved in governance of the DAO, other crypto-asset holders, or users of protocols that the DAO is associated with. DAO distributions can occur through private sales, vesting and liquidity mining, as well. Once issued by a DAO, DAO tokens typically can be traded for other crypto-assets on DEXs, deployed into DeFi protocols, and often are traded on CeFi crypto-asset trading platforms.

In theory, a DAO's governance rules could be encoded in smart-contracts on the blockchain on which it depends and all on-chain activity associated with a DAO could be immutably recorded on the blockchain, providing transparency to observers.[120] In practice, however, DAOs rely critically on input from human actors for their operation, including through activities that occur off-chain. DAOs often are accompanied by their own foundational documents that describe the goals of the DAO.[121] Some of those foundational documents have been described as constitutions, covenants, manifestos, charters, codes of conduct, and guidelines, among other descriptions.[122]

As it is costly to record every action to a blockchain, much of a DAO's activities typically occur off-chain. Off-chain communication tools are used to increase efficiency, facilitate onboarding, discuss proposals, and come to an agreement with members to achieve their goals.[123] The most popular communication tools used by DAOs today include popular social media platforms. Each of these services have varying terms of service and features. Thus, contrary to widely made assertions, while a DAO may involve elements of governance carried out by smart contracts on a blockchain, it also includes off-chain governance involving human interaction and negotiation.[124]

DEFI VOTING STRUCTURES

A major tenet of DeFi is to eliminate reliance on centralized institutions, including centralized governance structures. Some DeFi entities attempt to effectuate governance in ways that claim to avoid centralized control and to flatten hierarchies. The stated effort is to spread power among a broad participant base. Proponents of DeFi assert that code can be deployed to obviate the need for traditional centralized governance mechanisms. Nevertheless, and notwithstanding new approaches to governance, it has become clear that control and decision-making authority in DeFi projects as a practical matter remain concentrated, and a relatively small number of participants may in reality exercise dominion over a DeFi project or protocol, including the ability to control or influence its operation.

[120] Some proponents of DAOs proffer that a DAO's activities can be managed completely on-chain so that anyone can observe its activities, audit its smart contract code, and participate - giving both investors and workers greater transparency and involvement into the inner workings of the organization, with the same opportunities to profit or benefit from its operations.

See https://github.com/metagov/constitution-template/tree/main/constitutions (a repository of DAO constitutional documents).

[122] *See, e.g.*, https://constitutions.metagov.org/article.

[123] Hatice Ugurel, *The best communication and consensus tools for DAOs in 2022*, MEDIUM (Apr. 12, 2022), https://medium.com/multytude/the-best-communication-and-consensus-tools-for-daos-in-2022-7a8a26134204.

[124] BlockScience, *Exploring DAOs as a new kind of institution*, MEDIUM (Mar. 31, 2021), https://medium.com/block-science/exploring-daos-as-a-new-kind-of-institution-755eb119996b.

As observed in DeFi as currently operating, governance mechanisms can broadly be described in two categories: social and algorithmic. Social governance mechanisms facilitate organization and communication across networks of people, often using social media tools and fora.[125] Algorithmic governance mechanisms program rule sets into code, smart contracts and DLT-based protocols, which will be executed by computer nodes performing functions across a DLT network.[126] In most cases, DeFi governance is carried out by some combination of social and algorithmic mechanisms. However, it is important to note that, while most DeFi projects claim to rely to a varying degree on algorithmic governance mechanisms, code itself is created and deployed by humans and requires ongoing human participation to effectuate maintenance, development and upgrades. The projects themselves also rely on social governance mechanisms.

Also, various activities within these two types of mechanisms – social and algorithmic – can and do occur on-chain and off-chain. For example, a governance proposal for a particular DeFi project may first be introduced to a community off-chain, on a project's website, or a social media forum. The proposal may then be posted to, discussed and iterated upon in an off-chain forum dedicated to project governance, and may be the subject of informal polling to gauge community sentiment.[127] In some cases, a proposal may need to secure sufficient support in an off-chain poll or vote in order to proceed further. Once a proposal has gained informal consensus, it may proceed to a formal voting process that can be implemented on-chain, off-chain, or through a hybrid model.

Governance (Voting) Tokens

DeFi projects often attempt to distribute governance through the use of crypto-assets that confer certain voting rights. These are often referred to as *governance tokens* or simply *voting tokens*. As described in more detail in the 2022 Report, DeFi projects – whether or not they are organized as DAOs – attempt to argue that the existence of these governance or voting tokens provide decentralized governance. Such claims, however, must be examined to determine how a particular protocol actually is managed and what voting rights any of the governance or voting tokens provide, and whether at the entity or at the smart contract level. The following section describes how governance tokens are being used

[125] *See Governance of Web3 Networks & Other DAOs*, GITHUB.COM, https://github.com/sherminvo/TokenEconomyBook/wiki/Governance-of-Web3-Networks-&-Other-DAOs ("Social governance refers to the human decision-making process over when and how to conduct potential protocol upgrades in a Web3 network or in the smart contract code of a DAO. It deals with the institutionalized decision-making process of how stakeholders in the network receive necessary information to make educated decisions about future protocol upgrades…. However, navigating in a sea of information, and evaluating the authenticity and credibility of that information and signaling is difficult.").

[126] 2022 Report, *supra* note 5, at 3 (for a discussion of "smart contracts").

[127] DeFi project sponsors may provide a forum for participant discussion and community feedback. Many projects use a template/white label forum service hosted under a specific project URL. *See, e.g.*, https://www.discourse.org. Project sponsors may also take the lead in soliciting feedback, coding specific proposals, requesting votes, and promoting adoption.

in DeFi. It identifies their role and uses, the technical aspects of how they function and their limitations, and also highlights potential risks that arise from their use.

As described in the 2022 Report, governance (or voting) tokens purport to confer certain voting rights on their holders (or a holder's delegated persons, if the voting rights can be delegated). Typically, voting tokens entitle their holder to participate in certain aspects of governance (e.g., to make proposals to be submitted to a vote of the members and to vote on proposals made by other members) and/or to share in any profits the project generates (typically through the use of the governance token in the protocol in some way).[128]

When a project determines it will use voting tokens, it can establish the rules of voting in several respects, including the type of voting structure. Voting tokens confer voting rights that may be exercisable only by the token holder or that may be delegable by the holder to another. Voting power may be proportionate to the number of tokens held, can be one vote per participant, or there can be some other form of voting structure, such as a representational or delegated voting structure, to combat a lack of continued interest in governance among many participants. Whatever the structure used, it is important to focus on what types of decisions vote holders can actually vote on, among other factors discussed above. Some common approaches to voting structures have emerged and are described in industry reports.[129]

First, ownership of governance tokens for any given project can be highly concentrated, either because the project initially distributed the tokens in a way that placed large concentrations in a single person or a group of persons, or because, due to the transferability of such tokens, certain entities then acquired significant shares of tokens, or voting rights relating to such tokens. Based on on-chain data, it appears that, for many DeFi projects, much of the voting power resides in a few wallets. Data also shows that governance token holders tend to be inactive in governance voting. The participation for most of the proposals reportedly involved less than 10% of the total outstanding supply of tokens.

[128] In order for a project that uses governance tokens to do this, at a minimum, the governance tokens must be widely distributed among project participants and grant them the actual ability to participate in the management of a project, and a dispersed community of those participates must actually participate in the management of the project through community voting. Examining publicly available data regarding current DeFi projects indicates that this is not achieved in practice and there are practical limitations to its achievement.

[129] Some of these structures are referred to as ***quorum*** (requiring a certain threshold of voters); ***permissioned relative majority*** (no minimum voting requirement); ***quadratic*** (modified form of ranked choice voting); ***conviction*** (based on the aggregated preference weighted by time); ***multi-sig*** (voters signal on proposals while a committee votes); ***liquid democracy*** (participants delegate their votes). *See e.g.*, Eric Arsenault, *Voting Options in DAOs*, MEDIUM (Dec. 15, 2020), https://medium.com/daostack/voting-options-in-daos-b86e5c69a3e3; *DAO Voting Mechanisms Explained [2022 Guide]*, LIMECHAIN (May 23, 2022), https://limechain.tech/blog/dao-voting-mechanisms-explained-2022-guide/.

Second, a project can have voting tokens that allow the voting rights associated with the tokens to be delegated, lent, or otherwise assigned, such that someone other than the token owner may, in fact, exercise the power to vote that token. Thus, regardless of voting token ownership concentration, voting power itself, through delegation, can be concentrated in a single person or a group of persons that may or may not have a direct financial ownership or other interest specific to that project.

Third, the types of decisions that can be voted upon with respect to any particular project vary and may be limited to those that do not significantly impact the management of the project, or the management of the entity creating or involved with the project. Certain fundamental features of a project's protocol may be fixed in the original protocol code and not subject to change or may be subject to the control of a single person or a small group of persons. Further, token holders and their votes may be treated as advisory guidance to a controlling person(s) rather than as a binding decision. Votes may merely ratify or accede to actions already taken that impact a DeFi protocol or project. It may be the case that a protocol's core developers, operators or other select participants retain the sole ability to change core aspects of a protocol, and that the scope of proposals that governance token voters can vote on is limited. In fact, the project organizers may minimize governance intentionally so as to ensure that a protocol's fundamental operation is not subject to change. This is a concept that has been referred to as "governance minimization" where protocols are designed to reduce the chance that a core aspect of the protocol will change in order to enhance the long-term dependability of the protocol, especially if it is "composable" (i.e., compatible) with other protocols or elements in the DeFi ecosystem. As composability is a feature of DeFi, allowing for developers to build upon open-source code and integrate with other protocols, a project may design its protocol so as to minimize ways that the core code of the protocol can be changed. In other words, in order to "trust" a particular protocol, a user typically would want to know that the protocol acts reliably, predictably and that someone would be accountable for any deviation. Governance minimization may also help protect a protocol from certain types of attacks. If, for example, governance token voters could use their power maliciously to access funds locked in smart contracts or change core terms to exploit a protocol, this would reduce the security and resilience of the protocol.

Fourth, a number of factors, apart from the ownership concentration, voting power distribution and the aspects subject to change by vote, may diminish the degree to which governance is decentralized. These include policies and procedures that have been set regarding the process for proposing project changes, voting on such changes (e.g., quorum requirements, nature of the vote, timing, etc.), and implementing those changes.

Analyzing Governance Structures

When analysing a DeFi project's governance structure -- whether or not it is organized as a DAO -- it is critical to understand who can change which aspects of the project and how. Determining how governance works in any particular DeFi project requires a careful assessment. In analysing governance/voting token structures, it is useful to determine, among other things:

- who issued the governance/voting tokens and how were they offered, sold and/or distributed, including to the core team, investors and the community, and whether there were any limitations to voting, such as by time-locks, thresholds, or other means;
- who controls the governance/voting token issuer and what type of entity is that issuer;
- who controls the funds of the issuer and how;
- what type of legal entity, if any, is used to enter into agreements, contracts and capital raises;
- which aspects of a project can be altered by token vote, and whether there are some aspects that only select individuals can alter (i.e., assigning and revoking powers delegated to the operator/core development team, creating budgetary proposals, changing core protocol parameters);
- who decides which aspects of the project can be altered by token vote, and whether and how this can be altered;
- whether there is a minimum threshold of token ownership or voting power for proposing a governance change, voting on a proposal, or passing the proposal;
- whether governance/voting requires additional technical functions, i.e., delegation or locking into smart contracts or *staking*;
- whether there are any limitations on who can vote on a proposal (all users/token holders, only governance/voting token holders, other token holders, or only the operator/core development team);[130]
- whether there are any individuals with any gatekeeping function, i.e., veto power, power over whether a proposal is put to vote, power over whether a proposal, if approved, actually is implemented;
- what is required to implement a particular proposal, i.e., whether the alteration is effected automatically on-chain or requires select individuals to implement, i.e., with an administrative key;
- whether there are aspects of the project that can be changed unilaterally by the operator/core development team (e.g., through an administrative key);
- in reality, how concentrated is the proposal, voting, and implementation power of decision-making; is the decision-making spread across a large group of disparate persons or is a smaller group of persons exerting actual control;
- What role do founders and/or developers play;
- Are any services being used to facilitate governance; and
- How are processes and the implementation of decisions automated.

In the use of governance/voting tokens for DeFi governance currently, there is significant interplay between an on-chain and off-chain governance processes, as they are not mutually exclusive and often are used in combination. For example, in a common scenario of DeFi governance: a high-level proposal is introduced and discussed in off-chain

[130] In certain DeFi protocols, besides a governance/voting token, there can be one or more other tokens used for its business and operations, such as an LP token, or a stablecoin.

communications on social media; an initial proposal is posted and discussed on an off-chain governance forum; a "signaling vote" is conducted off-chain (usually with no token required); if the proposal passes the signaling vote, the proposal is posed to, for example, Snapshot for a vote off-chain (a token may be required to participate); if passed, a final vote is conducted on-chain (token is required to participate).[131] Thus, during a typical voting process, off-chain voting may or may not require that a voter hold a voting token, while on-chain voting usually permits only those with the private key associated with each of the tokens the ability to cast a vote, usually in proportion to the quantity of governance token held (unless voting power has been delegated to another).

DeFi governance generally is not self-implementing and human involvement typically is necessary to effectuate governance decisions. At a minimum, proposals to make any changes to a project's protocol, smart contracts or code must be translated into usable code and implemented, so those with governance control often must rely on others with technical control and skill (i.e., administrative access and requisite technical capability).[132] [133] Even for pre-programmed governance actions that are programmed to be implemented autonomously by means of a smart contract or other code, intervention by those with administrative keys may still be necessary. Those with an administrative key may retain the power to intervene or halt pre-programmed actions that have been approved by the voting community. In addition, with respect to ongoing governance through a community proposals process, some DeFi projects may use governance facilitators, who act as gatekeepers for advancing any new proposal to an on-chain vote. Depending on who these individuals are, how they are selected, and what accountability they may have, the use of governance facilitators may result in de facto centralization of control.

Finally, where a token holder keeps their token can impact their ability to vote. For example, if a token holder deposits their tokens into a certain hosted wallet or smart contract, the holder may lose their ability to use the tokens to vote while they are in the wallet or smart contract.

<u>Common DeFi Governance Proposal Characteristics</u>

The following lists typical characteristics of common DeFi governance proposals. The list does not necessarily describe any particular DeFi arrangement in operation today; rather,

[131] *See What is Blockchain Governance: On-Chain vs. Off-Chain*, PHEMEX ACADEMY (Oct. 13, 2021), https://phemex.com/academy/what-is-blockchain-governance (describing the Ethereum Merge, noting potential impacts that Proof of Stake (PoS) may have on use and implementation of governance tokens and suggesting that on-chain process may become more formalized as it is easier to do in PoS model).

[132] In some cases, proposals can be "pre-programmed", and by means of a smart contract, may execute if a vote succeeds. Even here, however, power may be reserved by an entity with technical control to nullify a proposal or otherwise stop its implementation.

[133] Conceptually a smart contract could be deployed to monitor governance votes and then automatically implement the will of the community. In practice, however, fully automated governance is unlikely as governance issues may not be foreseeable.

it is drawn from features of existing DeFi arrangements and seeks to capture and illustrate common and prevalent features and activities pertaining to the listed categories.

<u>Characteristics of Proposal Origination:</u>

- Project Change Process
  - On-chain
  - Off-chain
  - Hybrid
- Eligibility of Proposals
  - Direct proposing
  - Approval by community poll
  - Chaperoned by project or community representative
- Eligibility to Proposing
  - No restrictions
  - Token gated online forum access
  - Token ownership threshold
- Proposal Vetting
  - None
  - By community in online forum
  - By selected committee or project leadership

<u>Characteristics of Voting Rights:</u>

- Eligibility to Vote
  - Token ownership
  - Token delegation
  - Token staking
  - Address whitelisting
- Vote Mechanism
  - Assigned to an address based on token ownership
  - Assigned to an address based on token delegation
  - Assigned to an address based on token staked
  - Assigned to an address based on whitelisting
- Weighting of Voting Power
  - No weighting
  - Weighting based on type of token owned
  - Weighting based on balance of tokens owned
- Location of Vote
  - On-chain
  - Off-chain
- Major Holders (As % of total token supply held by a single address)
  - e.g., 25% to >40%
- Treasury Tokens (As % of total token supply)
  - e.g., 8% to >30%

<u>Characteristics of Voting Process:</u>

- Voting window
  - Total number of votes
  - Quorum threshold
  - Time limited
- Proposal Execution
  - On-chain, automatic
  - On-chain, automatic with time-lock
  - On-chain, manual with multi-sig
  - Off-chain, manual with development
  - Off-chain, manual with committee approval
- Quorum requirement
  - None
  - e.g., 2% to 20% varying on type of change
- Observed typical participation rates
  - e.g., 0% to <20%
- Emergency approval process
  - None
  - Emergency shut down or freeze
- Number of Proposals Voted on
  - e.g., 0 to >500

<u>Characteristics of Vote Impact:</u>

- Stated intent of vote
  - Non-binding
  - Temperature check
  - Signaling
  - Ratification
  - Binding
- Time-lock before execution
  - None
  - e.g., 1 to 7 days
- Emergency shutdown
  - None
  - Yes, through voting
  - Yes, through multi-sig
  - Yes, through admin or guardian rights

<u>Characteristics That Can Be Voted On</u>:

- Protocol parameter changes
  - Interest rates
  - Fees
  - Supported assets

    - Changes to tokenomics
    - Upgrades to the codebase
- Project operations
    - Key personnel
    - Committee structures
    - Multi-sig ownership
    - Deployment to new blockchains
    - Deployment of supporting infrastructure
- Treasury
    - Distribution of funds for operations
    - Distribution of funds for grants
    - Distribution of funds for individual use

Characteristics of Proposal Implementation Gatekeeping:

- On-chain
    - Time-locks
    - Admin and guardian rights
    - Deployment of new smart contracts
    - Disbursement of funds if digital asset
- Off-chain
    - Manual development
    - Appropriate development repository access
    - Disbursement of funds if fiat currencies

ANNEX E – UPDATE TO RISKS AND CONSIDERATIONS RELATING TO DEFI ACTIVITIES

The 2022 Report set forth many of the risks relating to DeFi activities, which persist today. This Annex highlights and gives more detail into certain risks that have been prominently illustrated by recent events and trends.

Risks Associated with DeFi Governance Structures

Specifically, since the publication of the 2022 Report, DeFi governance structures have continued to evolve, as discussed further in **ANNEX D**. Below are some of the key risks to investor protection and market integrity that arise as a result of common DeFi governance structures, in particular DAOs and governance/voting tokens, used individually or in combination.

Pseudonymity/Anonymity

The pseudonymity and anonymity[134] that are enabled through the use of DLT pose several unique risks when using DeFi arrangements and services that employ distributed governance mechanisms. These include:

- **Unknown counterparties and affiliates:** Typically, anyone can engage with DeFi protocols by purchasing or otherwise acquiring tokens, and token holders are not required to verify their identity, through anti-money laundering (AML)/know your customer/client (KYC) procedures or otherwise. As such, participants' real-world identities are not generally known to one another. As a participant in a DeFi governance mechanism through, for example, membership in a DAO or holding voting rights through governance/voting tokens, the participant may not be able to verify with whom they are interacting, which may put them at risk in terms of engaging with illicit finance actors, among other risks.
- **Lack of visibility into actual control**: The pseudonymity of blockchain transactions and the opacity into off-chain communications make it difficult if not impossible for investors or users to know exactly who controls a specific DeFi project and how decentralized that control is.[135] What might appear to be dispersed activity

[134] Typically, transactions occurring on public and permissionless blockchains are pseudonymous, that is, public blockchain addresses may be known and transactions associated with a particular address may be observable using blockchain explorer and analytical software, but the identity of the persons engaging in transactions is not known without additional attribution information. This pseudonymity is possible because of the public/private key cryptography that underlies public blockchains. Furthermore, certain anonymity enhancing technologies, such as anonymity-enhanced crypto-assets, mixers, and other techniques, are sometimes employed to make those persons and/or their transaction details unknowable.

[135] Governance/voting tokens typically are traded on centralized crypto-asset platforms, and therefore significant amounts of them may be held in omnibus wallets belonging to the platform. Thus, it is impossible to know through public address analysis alone the level of concentration among holders

could in fact represent the actions of a single actor or a group of coordinated actors. The ownership and voting of governance/voting tokens, including those of DAOs, typically are unknown to the broader collective of voters and/or members.[136]

- **Voting rights and the actual ability to participate in the governance of a DeFi project may be illusory:** Aside from ownership and votership concentration, the ability to participate in governance through voting relies upon a number of factors that essentially depend upon how the issuer has established the governance mechanism, including determining which aspects of the enterprise are up for vote, and the policies and procedures around voting. This includes whether a central actor(s) has any *gatekeeping* role over the governance process, such as through holding an administrative or guardian key. In some cases, governance proposals may be required to be submitted in coded form, creating significant barriers to participants who are unable to do so.
- **Conflicts of Interest and Collusion**: Due to pseudonymity, it is difficult to verify what conflicts of interest exist between various market participants, what conflicts have been disclosed, or the effect of conflicts on other market participants. As a result, it is difficult to ascertain whether large voters – who may or may not have an ownership interest in a project and are voters by virtue of delegation – are acting in their best interest or in the interest of the project. Further, there may be off-chain, privately communicated efforts to influence token holders and voting delegates. There is also a lack of transparency when it comes to the delegation of voting power where large token holders (whales, venture capitalists (VCs), institutional investors, voting consortia) can have concentrated voting power and can obfuscate their voting activity and control.

<u>Information Asymmetries</u>

Information asymmetries in the context of governance/voting mechanisms, regardless of which technological tools DeFi projects use to coordinate and communicate, can arise from a lack of even-handed communication among members, such as through the

of such tokens. In addition, voting rights may be separable from a governance/voting token ownership such that ownership alone is not a proxy for voting distribution. Further, depositing a governance/voting token in a smart contract or on a platform may mean that it cannot be voted. Furthermore, off-chain activity, such as private communications, could obfuscate concentrations of power, such as through outsized influence of particular actors or collusion, as it would not be visible for participants to monitor. Thus, what seems like community-driven voting could in fact be centralized management. This can occur if, among other reasons, governance/voting tokens are held by a concentrated actor or actors, if voting power is held by a concentrated actor or actors, if a majority of those with voting power are not in fact voting (voter apathy), or if a central actor or actors has control or sufficient influence.

[136] While on-chain data does provide some information with respect to public addresses that hold governance/voting tokens, it is impossible to know – without additional attribution data -- who the beneficial owners of addresses are or whether certain addresses belong to the same beneficial owner or related parties.

restriction of access to communication channels.[137] Information asymmetries could result in the non-disclosure of important information to all governance/voting token holders, enabling potential insider- and self-dealing, and fraud or misappropriation of assets.[138]

Cyber Exploits/Attacks

In addition to general cyber risks involving the use of DLT, risks to governance could also occur due to code vulnerabilities or exploits. For example, attackers have used "flash loan attacks" (see the 2022 Report and **ANNEX B**) to obtain a majority of a DAO's voting tokens in order to drain some or all of the assets from the DAO. Administrative keys that control certain functions of smart contracts can be leaked or "hijacked." Poor logic or coding errors in a protocol have been exploited.[139] As noted in the 2022 Report, there could be a "Sybil attack" in which certain individuals with advanced knowledge of a governance/voting token "airdrop" could generate multiple pseudonymous addresses to obtain control over a concentration of airdropped tokens to gain influence over a project. In each of these scenarios, the governance process of a DeFi project can be impacted. Even in the absence of an attack on a particular DeFi project, as DeFi is blockchain-based, any disruption or failure of a blockchain that underpins a particular DeFi product or service -- including any congestion, forks, attacks or nefarious activity -- likely will directly impact the operation of a DeFi governance structure. Furthermore, if fees increase on a particular blockchain (e.g., due to congestion), this can impact the practicality of voting for some participants.

Legal Compliance

DeFi projects may be operating outside of, or in non-compliance with, legal frameworks that apply to the activities they are conducting, such as applicable securities and other financial markets laws. As a result, investors and users in DeFi projects, including those involving governance tokens, are not getting the protections that those legal frameworks provide. These protections include protections against fraud and manipulation. Furthermore, investors and users may not have any claim or redress for improper conduct under private rights of action. Legal uncertainty and risk of loss is exacerbated by the cross-border nature of DeFi arrangements.

Governance Token Proposal and Voting Risks

Unlike traditional corporate structures with legally clear lines of responsibility, the legal obligations of participants in structures such as DAOs may be unclear in many jurisdictions. As a result, in any particular jurisdiction, it may be unclear what recourse there could be for any particular token holder for the action or inaction of other token

[137] Restriction of access can occur through settings of on-chain communication platforms or through restrictions to off-chain communication platforms based on token ownership (token-gating) where software verifies token ownership in a wallet prior to granting access to information.

Spencer Graham, *Community Contribution Opportunity*, HAUS PARTY, Jan. 4, 2022, https://daohaus.substack.com/p/community-contribution-opportunity.

[139] *See. e.g.*, Greg Noone, *Can DAOs survive an onslaught of cybercrime?*, TECHMONITOR, July 21, 2022, https://techmonitor.ai/focus/daos-cybercrime-dao-hacks.

holders, or of the DAO. For example, there may be no obligation of managers or others holding significant amounts of governance tokens to act for the benefit of other holders or any limitations on their use or sale of governance tokens. Moreover, once developers monetize their investment through, for example, the sale of their own governance/voting tokens, they may lack the incentive to continue to develop and maintain the protocol.

In addition, a voter who may hold voting rights only through a voting delegation (and not ownership rights) could thereby influence the protocol without any interest in the long-term prospects of the protocol. In any event, a voting community could become polarized over voting decisions, which could lead to significant disruption, forks or network splits, or losses in confidence – all posing risks to holders of governance tokens or participants in the DeFi ecosystem.

Implementation Risks

There are also risks relating to implementation of software code changes approved through governance actions. DeFi protocols are, at least in part, software code. Software typically requires consistent maintenance and upgrade in order to perform optimally. Without such upkeep, software can fail due to compatibility issues, code vulnerabilities, hacks or other operational problems. The code of a protocol and its associated smart contracts may not function as intended or may react in unexpected ways over time as new circumstances emerge that were not anticipated. This raises some key risks relating to governance/voting token structures.

For example, in the event of a software issue, the viability of a DeFi project (and safety of user assets) may depend upon the ability of project participants to identify the issue, develop and code a solution, and marshal the voting apparatus and consensus around necessary protocol changes, often in an expeditious manner. This process is dependent upon many factors, including humans with the technical skills required to propose and code the upgrade, and voter interest and participation to follow through with what is required to approve and implement the proposal. An absence of participants who possess the technical capability, skills and know-how in relation to the coding of a protocol, or an inability to obtain required votes, each raise questions about the timeliness and effectiveness of governance processes. These issues also raise questions of key-person risk, and also that of accountability (e.g., who is responsible for untimely and ineffective governance resulting in failure of a protocol or harm to its users or others).

Risks Associated with Levered Strategies in DeFi

Highly levered products currently are being marketed to and are available to investors through DeFi projects. As a result, investors, including retail investors, are exposed to a number of risks:

- Access to leverage that is higher than on regulated markets, with the potential to magnify losses beyond which the investor can bear;
- Increased exposures to speculative assets that may lack fundamental value (i.e., do not contribute to broader social or economic function and, relatedly, reduction in investment to those that do);

- Substantial product complexity given the terminology used to describe such products (e.g., perpetual futures) and the magnitude of leverage offered;
- Automated liquidation of positions;
- Increased speed by which a position can be liquidated due to the magnified leverage;
- Significant collateral commitment, particularly as leverage increases;
- The potential for traders to access unlimited leverage via leveraging spirals on a lending protocol;[140]
- The use of protocol-issued tokens that can then be used as collateral for levered positions, resulting in a form of self-collateralization and encouraging the creation of 'asset bubbles'; and
- Amplification of the high price volatility of the underlying asset due to high leverage and interlinkages resulting in procyclicality.

Excessive leverage can increase both volatility of asset prices and risks for financial stability overall by amplifying procyclicality. To mitigate against default risk, DeFi protocols rely on over-collateralization of positions and automated liquidations in the event that the position held by the trader breaches margin requirements. If these products were developed and used at large enough scale, there are potential systemic impacts arising from liquidation risk as automatic liquidations triggered by price volatility (or a shock to one part of the DeFi ecosystem) can have a procyclical impact on prices, impacting other DeFi protocols or crypto-asset markets generally. Unlike regulated derivative markets there are no countercyclical buffers for DeFi protocols.

Further, the interoperability and interconnectedness of DeFi projects and protocols allows highly levered actors to use their debt as collateral in other protocols, which spreads risk across the system and creates an inherent risk of a system-wide run on assets.

<u>Risks Associated with Liquid Staking</u>

The use of derivatives and risks associated therewith are covered in the 2022 Report. One type of derivative that has emerged since the 2022 Report results from *liquid staking*. Typically, in proof of stake (PoS) network, staked tokens cannot be used for anything else while enabling a validator to participate in the PoS consensus mechanism for the opportunity to earn staking rewards. Liquid staking has developed as a way for holders of crypto-assets that are locked up in PoS consensus activities to continue to be able to use their tokens in other DeFi activities such as trading, lending, or as collateral. Specifically, liquid staking is marketed as a way of participating in PoS validation activities while addressing the lost opportunity cost of locking up staked tokens and, in some cases, overcoming the various thresholds to staking, which can include factors such as minimal amount of tokens to activate a validator, costly hardware, or technical IT expertise. Liquid staking service providers often offer a user the ability to earn multiple tranches of rewards,

[140] For example, a user can pledge ETH in one DeFi lending protocol in exchange for the protocol's stablecoin which he or she can then pledge on another DeFi protocol in exchange for a different stablecoin, and the process can be repeated indefinitely and is only limited by the level of the collateralization ratio of the lending protocol for assets pledged as collateral.

including a portion of block rewards, transaction fees, and any maximal extractable value (MEV) generated through participation. According to one blockchain analytics firm, liquid staking is the most popular method for participating in Ethereum staking, the largest PoS blockchain network.[141]

In liquid staking, a crypto-asset holder deposits their crypto-assets with a liquid staking service provider in exchange for another crypto-asset commonly referred to as a *liquid staking derivative* (LSD, also sometimes referred to as a *liquid staking token* or LST or *wrapped staked tokens*). In many arrangements, the LSD token can be transferred freely to be used in other DeFi activities such as for trading or collateral in another DeFi protocol for lending or borrowing activities to continue to earn yields and eventually can be used to redeem the staked asset if redemptions are available.

Liquid staking providers can also lower the threshold amount of crypto-assets needed to participate in PoS validation activities if minimal thresholds are required. The most common example is overcoming the 32 ETH minimal threshold to activate a validator on the Ethereum PoS network. Liquid staking providers can enable users to deposit less than 32 ETH into the protocol which then pools customer funds together and divides them into 32 ETH batches to activate validators. Liquid staking has grown significantly since Ethereum's Merge event that changed Ethereum from a proof of work (PoW) consensus to PoS consensus blockchain network. Since the Merge event in September 2022, there has been significant growth in the DeFi liquid staking market, growing from approximately 4.6M ETH on September 15, 2022 to approximately 9.4M ETH in June 2023.[142]

The mechanics and governance of liquid staking can change depending on the service provider and whether the service is provided through a centralized trading platform (CEX) or a DeFi platform. CEXs can provide LSDs in various manners, either restricted to use on the CEX platform or transferable off of the platform to be used in other activities such as DeFi activities mentioned above and are not likely subject to the DAO governance structure challenges described above. CEXs may or may not require the use of smart contracts to pool and manage users' deposits and withdrawals, deposit funds to node operators, determine fees, manage LSD token supply and other operational activates.

DeFi liquid staking services can also be organized and governed as DAOs and subject to the DAO governance structure challenges described above. DeFi platforms and related DAOs may rely on one or more smart contracts that typically pool and manage users' deposits and withdrawals, deposit funds to node operators, determine fees, manage LSD token supply and other operations activates. In addition, smart contracts can contain a full list of node operators, their public keys, and reward distribution records.

[141] https://dune.com/21co/ethereum-staking-and-withdrawals

[142] See id.; https://21shares.com/research/onchain-insights.-

Liquidity Staking Token Designs

In exchange for depositing staked assets into liquid staking protocols, the protocols issue users another liquid token, an LSD, representing their claim on the staked assets. The liquid asset commonly comes in two different token designs: (1) rebasing assets and (2) value-accruing assets.

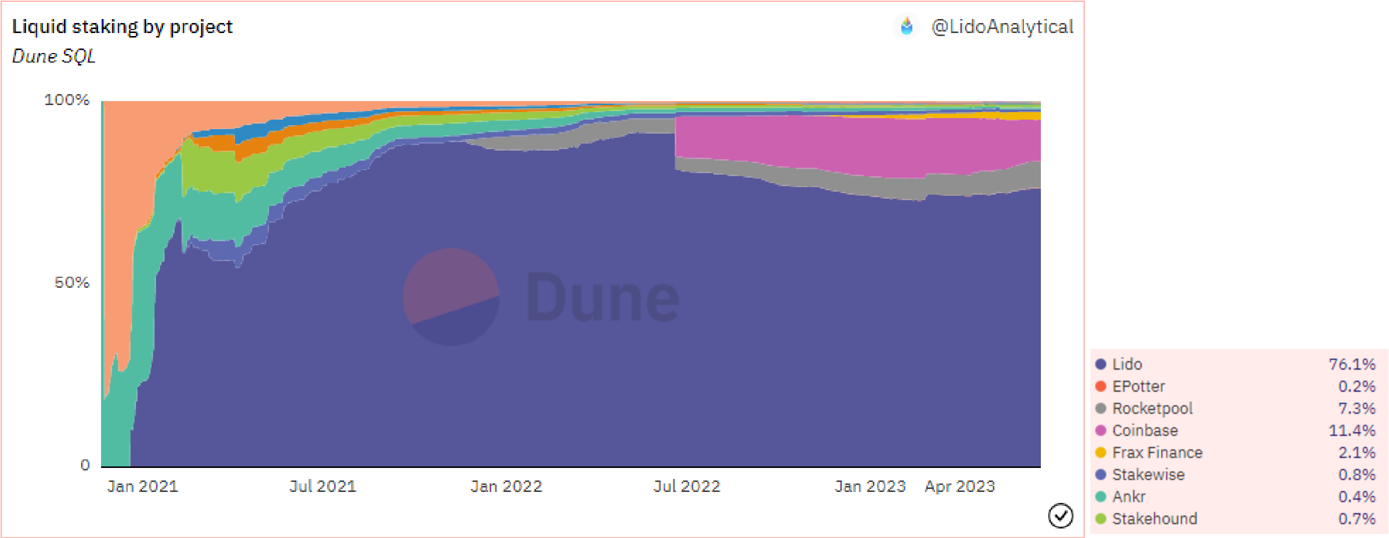
- Rebasing LSD assets are typically minted at a 1:1 ratio with the deposited crypto-asset. In order to match the underlying deposit plus any accrued rewards or deducted penalties, the token balance updates or *rebases* every day, via an oracle, to calculate rewards and penalties. The daily rebase occurs regardless of where the LSD is acquired; whether it is directly acquired from the protocol, a DEX, or another holder. A wrapping service, similar to Wrapped ETH, is used to enable interoperability of rebasing LSDs with other DeFi protocols.
- Value-accruing LSD assets are typically minted at a 1:1 ratio with the deposited crypto-assets. In order to match the underlying deposit plus any accrued rewards or deducted penalties, the exchange rate between the LSD and the underlying funds changes over time. The value-accruing LSD tokens typically have rights to the underlying staked assets plus rewards minus fees and rely on redemptions of the underlying assets to realize the accrued value. Value-accruing LSD tokens typically do not need wrapping services to be used in DeFi activities.

There are a number of risks that arise in liquid staking, some of which are not unique to DeFi or liquid staking activities. These risks include, but are not limited to, the following:

Liquid Staking Concentration of Validators Risk

Liquid staking concentration risks can occur at the validator node operator level where validation of transactions occurs, introducing risks to a PoS blockchain and risks to the users and protocols using the PoS blockchain. Some DeFi liquid staking protocols select a set of node operators that will be responsible for validating transactions using users' deposited crypto-assets that have been pooled by the protocol, in an off-chain process, sometimes decided by a committee. An opaque, off-chain selection process by a committee or a small group can create centralization and possible collusive, manipulative, or censorship behaviors. Concentration of validator nodes can impact the functionality of a PoS blockchain and represent significant consensus risks of a PoS blockchain if a single liquid staking protocol was able to exceed critical consensus thresholds, such as 33% of a network's validators, for an extended period of time. More specifically, an Ethereum researcher recently expressed concerns that if a liquid staking protocol reached critical consensus thresholds, controlling as little as one third of validator nodes, the liquid staking protocol managers could achieve outsized profits compared to other node participants via coordinated MEV extraction, block-timing manipulation, and/or censorship of block space.[143]

Lido currently dominates the liquid staking market for Ethereum holding more than 75% of the total market share.[144]



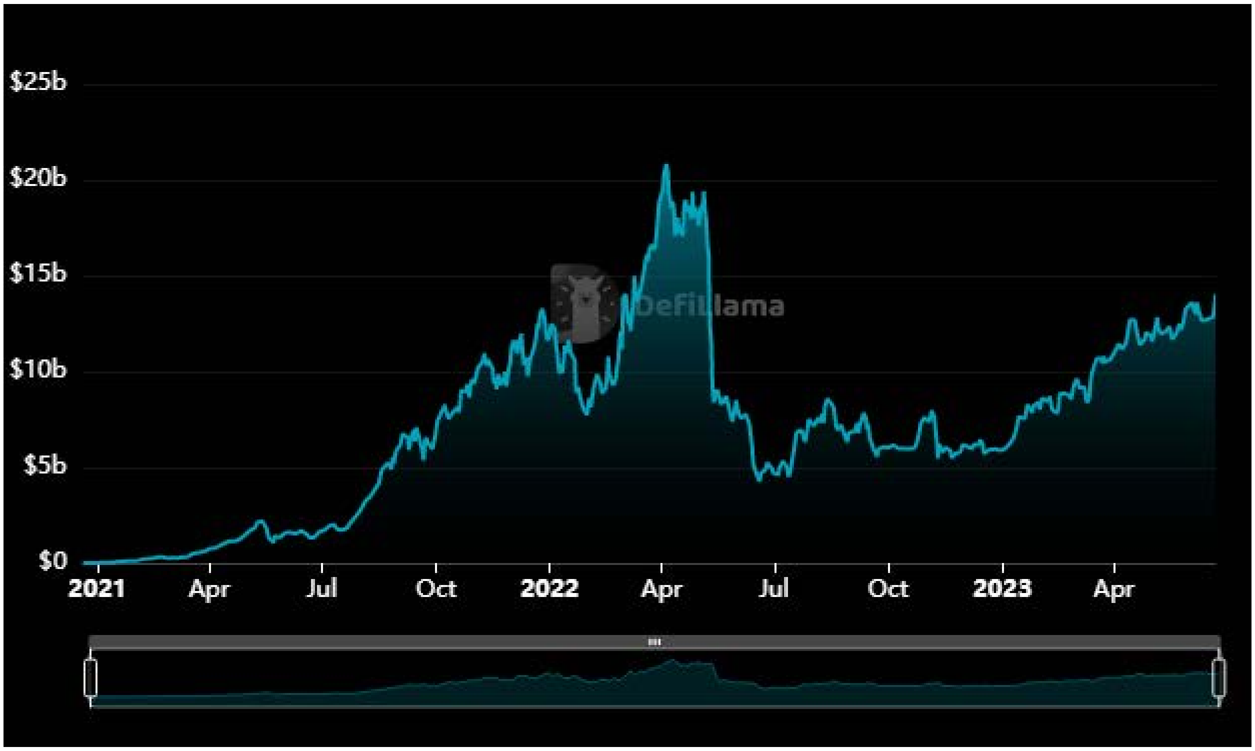
Source: Dune Analytics

Lido's TVL, in excess of $14B, is greater than the TVL of the second and third largest DeFi protocols, MakerDAO and Aave, combined.[145]

[143] *The Risks of LSD*, ETHEREUM, https://notes.ethereum.org/@djrtwo/risks-of-lsd.

[144] https://defillama.com/protocols/Liquid%20Staking.

[145] https://defillama.com/chain/Ethereum?tvl=true.



Source: DeFi Llama

Smart Contract Risk

Smart contracts add additional risk to the underlying IT operational risks inherent to running validator nodes. Many liquid staking protocols rely on smart contracts to facilitate their operations, LSD tokens, and governance. These smart contract operations can include functionality such as pooling users' funds, batching users' funds, sending users' funds to validators, issuing LSDs, managing LSD token supplies, redeeming LSDs for deposited assets, setting protocol fees, managing node operators, and managing certain governance mechanisms via a DAO.

These smart contract-facilitated operations can introduce previously discussed smart contract risks such as code errors, private key compromises and reentrancy attacks, among others. Even to the extent users' staked assets are locked in a smart contract, a provider could still have access to those assets through, for example, a private key with elevated administration rights. Even if there is no such key, the user is exposed to the risk that assets may be lost through a failure or attack on the underlying protocol or smart contract. These risks can exist at the smart contract level, protocol operational level, LSD token issuance level, and at the governance level if there is a DAO.

DAO Governance Risk

Many liquid staking protocols are organized as or governed by DAOs, offering associated governance tokens and voting structures to determine the direction of the protocol the DAO controls. DAO governance tokens can commonly be bought and sold on both CEX and DEX venues. DAO governance tokens can be susceptible to concentrations of voting power and control by a small number of early and/or large investors who own a significant supply of governance tokens or are delegated voting rights, if enabled by the governance token. Other risks of DAO governance are discussed above.

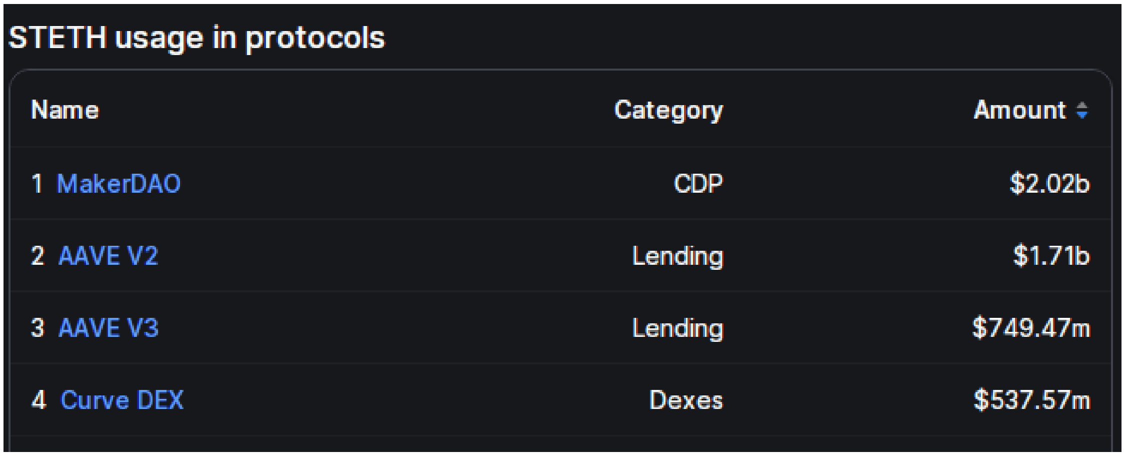
Redemption Value and Counterparty Risks to User

As with CEX liquid staking arrangements, users participating in a DeFi liquid staking arrangement are subject to redemption risk stemming from a variance in value between the LSD and the value of the staked crypto-asset, the exchange rate, which could impact a user when the user redeems the liquid staking token for the staked token.[146] This can occur if, for example, there is a decline in the value of the liquid asset relative to the staked asset (as it may have less liquidity or less uses, e.g., it cannot be used to pay gas fees). It could also result in an arbitrage event, where the price of a LSD is worth more than the underlying staked assets and redemptions or withdrawals are available.

Counterparty risk also exists to the other DeFi protocols that support LSDs as collateral for lending, trading markets, or other activities. For example, the top four usages of Lido's LSD token, *stETH*, occur in other DeFi protocols offering lending, collateralized debt positions, and swapping at, for example, MakerDAO, Aave and Curve Finance.[147] As observed in reports concerning the collapse of Terra Luna and crypto-asset hedge fund Three Arrows Capital (3AC), LSDs used as levered collateral in other DeFi arrangements can result in liquidations and contagion if the redemption value diverges from its 1:1, or more in the case of a value accrual token, ratio. In some cases, DeFi protocols reportedly have taken emergency action, using elevated administration rights to manage potential contagion risks. It is important to note that many liquid staking providers are CEXs and therefore a user is still exposed to various counterparty and other risks when depositing assets with a provider.

[146] For example, in June 2022, Lido's stETH deviated from the price of ETH due to a liquidity crisis in crypto-asset markets that led 3 Arrows Capital (3AC) reportedly to withdraw 80,000 stETH from DeFi protocols and convert back nearly 39,000 stETH at around 5% discount from ETH.

[147] https://defillama.com/tokenUsage?token=steth.



STETH usage in protocols

Name	Category	Amount
1 MakerDAO	CDP	$2.02b
2 AAVE V2	Lending	$1.71b
3 AAVE V3	Lending	$749.47m
4 Curve DEX	Dexes	$537.57m

Source: DeFi Llama

Risks Associated with Other Emerging Derivative Protocols

Several additional derivative protocols have gained popularity since the 2022 Report, presenting significant risks to retail investors to whom the protocols are marketed.

Perpetual Swaps:

A perpetual swap contract allows an investor to gain synthetic levered exposure to a reference asset, such as bitcoin or ether, without expiry of the contract. Perpetual swap contracts have become popular with some crypto-asset investors, as they seek high degrees of leverage and adequate liquidity through decentralized exchanges. A primary concern with these swap contracts is counterparty risk; decentralized platforms aim to obviate this risk by using automated market makers.

Automated market makers create liquidity pools of popular crypto-assets that allow users to purchase long or short perpetual swaps by connecting a crypto wallet. Decentralized exchanges offer a variety of crypto perpetual swaps, or futures, assuming adequate liquidity pools can be established. In addition, decentralized exchanges offer different levels of leverage, sometimes in excess of 30 times margin. Decentralized exchanges may rely on oracles to generate pricing or use an order book that allows buyers and sellers to generate price discovery.[148] Trading in an order book may require users to pay or receive a funding rate to incentivize participation on each side of the market (i.e., long and short).
Investors in perpetual swaps face significant risks, including:

- Complexity of the transaction and exchanges, given the differences in exchanges offering such contracts, and the varied terminology used in marketing such arrangements. For example, perpetual swaps or futures can be liquidated much more quickly than many futures terms given their heightened leverage and the volatility of the underlying reference asset.

[148] *See* dYdX Trading, Decentralized, https://dydx.exchange/?.

- Leverage on swap contracts that may prohibit users from holding a contract for a period of more than a few minutes[149] without the possibility of full loss depending on the volatility of the reference asset.
- Deviation of contract pricing from the reference asset's spot market depending on the accuracy of the oracle or depth of the order book.
- Fee transparency is difficult to ascertain given the diversity of exchange structures;
- Significant fees associated with maintaining a position or associated with the funding rate, depending on the depth of the order book.
- Significant collateral commitment, particularly as leverage increases.

Synthetic Crypto-assets:

Decentralized exchanges offer synthetic crypto-assets or fiat currencies to users via derivative tokens. These synthetic assets may be used for a variety of purposes, including trading with leverage, for deposit into a pool to earn yield, or to collateralize options.
Investors in synthetic crypto-assets or fiat currencies face significant risks, including:

- Deviation of pricing from the reference asset spot market depending on supply and demand of the synthetic instrument.
- Counterparty risk to the issuer of the synthetic crypto-asset.
- Platforms are designed to allow the creation of synthetic assets that combine derivative positions.
- Procyclicality of derivative instruments referencing the underlying performance of derivative instruments.

Options on Crypto-assets:

Certain protocols use AMMs to offer options in crypto-assets, such as ETH or wBTC, to users. Users are offered a variety of puts and calls to buy or sell at different strike prices and expiration dates. Liquidity is maintained in the pool by liquidity providers who deposit crypto-assets to a market-maker vault; these liquidity providers earn fees when options are traded.
Investors in options on crypto-assets face significant risks, including:

- Complexity in crypto-asset option markets, including the historically strong variance between spot and futures prices.[150]
- Reliance on oracles to determine pricing at expiry.
- Liquidity providers may be subject to withdrawal risk in which they must wait for their funds until adequate liquidity is achieved in a specific pool.
- Unexpected or unanticipated interactions between traders and liquidity providers. For example, a sustained win rate for traders might result in losses for liquidity providers.

[149] *Id.*

[150] Maik Schmeling et al., *Crypto carry*, (BIS Working Paper No. 1087, Apr. 2023), https://www.bis.org/publ/work1087.pdf.

Risks Associated with Oracles

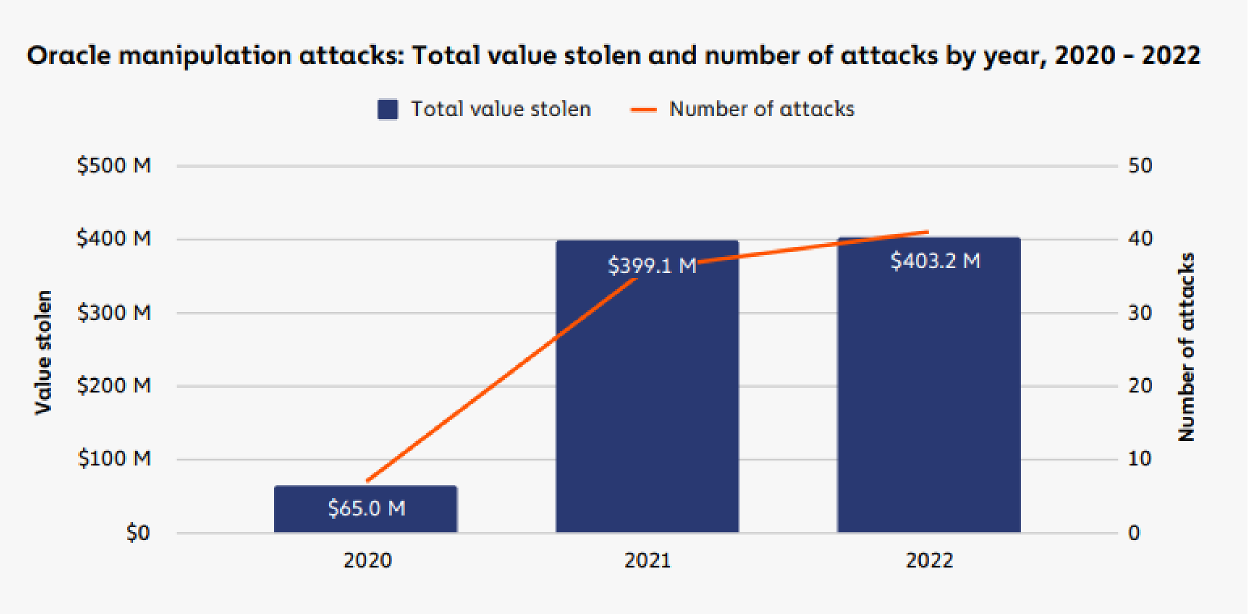
When a protocol relies on an oracle for data, such as pricing data, there is significant risk if the data is inaccurate – whether due to manipulation, deprecation, or other reasons.

Risk of Manipulation

DeFi protocols often use pricing oracles to provide information to trigger margin calls, liquidations or to settle positions. These pricing oracles can be centralized or they can claim to be decentralized. A centralized oracle is controlled by a single entity and can be the sole source of information for the DeFi protocol. Centralized oracles have a single point of failure which can mean these protocols are vulnerable to corruption and attack.

An asserted decentralized oracle typically sources information from multiple nodes across the oracle network to confirm the underlying source data. The source data can be market data from one data source, such as a centralized crypto-asset trading platform, or data from multiple centralized crypto-asset exchanges, e.g., for the market price of a crypto-asset. As is the case for centralized derivative protocols, there is potential for decentralized oracle data to be manipulated by bad actors. The effect of oracle price manipulation is comparable to benchmark manipulation and can result in harm to users of the protocol. In addition, the decentralized oracle is established by code, and subject to the same issues and risks as other code used in DeFi protocols.

One blockchain analytics firm estimates that DeFi protocols lost $386.2 million in 41 separate oracle manipulation attacks.[151]



Source: Chainalysis – The 2023 Crypto Crime Report.

[151] CHAINALYSIS, *supra* note 21.

Typical Oracle Attack

A typical oracle attack is based on the following steps and involves the use of a flash loan:

1. **Preparation of funds** – the attacker borrows a large number of crypto-assets via lending protocols.
2. **Raising the price of target assets** – the attacker manipulates the price of target assets (i.e., by exchanging many tokens back and forth between different liquidity pools). The oracle(s) relied upon by a DeFi protocol pass the manipulated price data to the DeFi protocol.
3. **Profiting** – the attacker exchanges the target asset for crypto-assets borrowed from the lending protocols. As the attacker inflates the price of the target asset, it can exchange the target asset for a larger amount of other assets.
4. **Loan repayment** – the attacker restores the assets in the liquidity pool to their initial state to avoid losses caused by price slippage and repays crypto-assets borrowed from lending protocols.

An oracle attack reportedly occurred on the bZx protocol when an attacker used a flash loan to inflate the value of a stablecoin (sUSD) on a decentralized exchange. The stablecoin was deposited into bZx as collateral at an inflated price, as bZx utilized pricing oracles from the decentralized exchange for the exchange rate of sUSD/ETH. This allowed the attacker to open an undercollateralized position utilizing the inflated value of the stablecoin as collateral and close out the position to withdraw more ETH than they otherwise would have been able to.[152]

Mispricing Risks

There is a risk of price divergence when the pricing data provided by an oracle diverge from the market price of the underlying asset. For example, price divergence could occur when there are market price dislocations on spot exchanges that feed into oracles or if the protocol does not update the pricing of its products in a sufficiently timely manner. High levels of volatility may exacerbate this risk as it may be inefficient for DeFi protocols to fetch pricing data from oracles on a real time basis due to transaction costs (i.e., gas costs) incurred[153] and block validation times[154]. In contrast, in traditional financial markets data feeds are normally provided on a near real-time basis.

[152] *The bZx attacks explained*, PALKEO (Feb. 18, 2020), https://www.palkeo.com/en/projets/ethereum/bzx.html.

[153] Oracles (or their node operators) may charge fees to provide data. *See, e.g.*, https://ethereum.stackexchange.com/questions/87473/is-chainlinks-price-reference-data-free-to-consume.

[154] For example, the protocol offered by Synthetix updates the smart contract pricing at fixed intervals (currently 3 minutes) based on the pricing oracle Chainlink, but only if any prices have moved above a particular amount.

Discrepancies between the oracle price or the price of the relevant crypto-asset and the unverifiable spot price of underlying assets, may result in a product not performing to the expectations of the user. There is also a risk that front-running attacks can be carried out by a user that pays a higher transaction fee so that their transaction is executed prior to the oracle price update.

Risks Associated with the use of Automated Liquidation Mechanisms

As noted above, many DeFi protocols, including lending and borrowing protocols and those that provide direct derivatives exposures, rely on over-collateralization and automated liquidations to manage default risk on crypto-assets issued. The effectiveness of the liquidation mechanisms used by these protocols is therefore paramount to the fair compensation of counterparties in the event of default.

Certain characteristics of the DeFi ecosystem can hamper the effectiveness of these mechanisms. For one, most smart contracts cannot liquidate collateral without an external party instigating the transaction. Protocols must either operate bots (automated programs) or incentivize market participants to purchase the collateral from them or otherwise instigate the liquidation process. These bots can be deployed to identify and profit from arbitrage opportunities if they identify deviations between the price quoted by the smart contract and the market price.[155] These mechanisms must be robust to a variety of market conditions. Any discount offered to market participants to incentivize liquidation must exceed any potential price depreciation of the collateral asset. This can be difficult as, in times of volatility, rising gas prices and elevated transaction volume can increase congestion on the network, meaning the prices at which the discount is calculated can be stale. Additionally, network congestion can result in gas prices exceeding the default tolerance that liquidation bots are configured to use, meaning that the transactions sent by the bots are not committed to the network. Some market participants and protocol operators have expressed concerns that a large enough collateral liquidation could prevent the entire underlying blockchain from processing transactions for some time.[156]

[155] *See* 2022 Report, *supra* note 5, at 15.

[156] ALEX MELIKHOV & PETER SERGEEV, EQUILIBRIUM WHITE PAPER 3 (2022), https://equilibrium.io/docs/zh/Equilibrium_WP.pdf.

ANNEX F – MAPPING OF IOSCO PRINCIPLES TO DEFI ACTIVITIES

Introduction

The 2022 Report detailed the operation of the DeFi ecosystem, discussing the technology components used, the various DeFi protocols for participants to engage in crypto-asset activities, the products and services provided in connection with such protocols, and the various participants in the DeFi ecosystem. The purpose of the mapping in this report is to examine and identify how typical DeFi products, services, arrangements, and activities implicate IOSCO Standards.[157]

This mapping is intended to identify how the IOSCO Principles should apply with respect to DeFi products, services, arrangements, and activities, based on a current understanding of the facts and circumstances, including the economic realities of activities in the DeFi ecosystem, first discussed in the 2022 Report.

In those jurisdictions where many DeFi participants are acting in non-compliance with existing laws, regulators can use this mapping to identify the activities and participants that already fall within the scope of their regulatory remit and to help assess how to apply their existing regulatory regime. In jurisdictions where existing securities and other relevant laws may not apply, this mapping can assist regulators as they consider ways to address any potential gaps in their regulatory regime. In both instances, the IOSCO Principles provide a sound basis for how to approach regulation of such activities and participants and avoid regulatory arbitrage between traditional financial activities and participants on the one hand, and DeFi activities and participants on the other. The mapping is not intended to accept existing arrangements and activities as static, without any ability or necessity for change. In fact, it is more likely that to comply with existing or new laws in jurisdictions, DeFi activities and participants may need to alter their operations. In addition, as most DeFi protocols operate cross-border it will be important for jurisdictions to cooperate as they assess the operation of the activities and participants in the DeFi ecosystem to avoid conflicting analyses and determinations regarding the application of IOSCO Principles.

A. Principles relating to the Regulator

1. ***The responsibilities of the Regulator should be clear and objectively stated.***

2. ***The Regulator should be operationally independent and accountable in the exercise of its functions and powers.***

[157] For all references to the IOSCO Principles in this report, see OICV-IOSCO, THE OBJECTIVES AND PRINCIPLES OF SECURITIES REGULATION (May 2017), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf. For further background on the IOSCO Principles, see OICV-IOSCO, METHODOLOGY FOR ASSESSING IMPLEMENTATION OF THE IOSCO OBJECTIVES AND PRINCIPLES OF SECURITIES REGULATION (May 2017), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD562.pdf.

3. ***The Regulator should have adequate powers, proper resources and the capacity to perform its functions and exercise its powers.***

4. ***The Regulator should adopt clear and consistent regulatory processes.***

5. ***The staff of the Regulator should observe the highest professional standards, including appropriate standards of confidentiality.***

6. ***The Regulator should have or contribute to a process to identify, monitor, mitigate and manage systemic risk, appropriate to its mandate.***

7. ***The Regulator should have or contribute to a process to review the perimeter of regulation regularly.***

8. ***The Regulator should seek to ensure that conflicts of interest and misalignment of incentives are avoided, eliminated, disclosed or otherwise managed.***

All of these IOSCO Principles relating to the regulator should apply with respect to DeFi activities and participants. A key consideration of the Principles relating to the regulator with respect to DeFi is whether the regulator has the appropriate resources – including knowledge, data and tools – to evaluate DeFi activities and participants. In addition, a significant challenge for a regulator in applying IOSCO Principles to DeFi is the limited availability and interpretability of verifiable data relating to many DeFi activities, and the resulting lack of transparency into those activities. Lack of transparency exists, in part, because information off-chain can be difficult to obtain and information on-chain can be difficult to interpret. For those activities that involve financial instruments, including securities, application of the regulator's existing regulatory regime will help address these transparency issues, as application of requirements will typically enhance recordkeeping and reporting. To the extent a jurisdiction may determine that the existing regulatory regime does not apply, the regulator could consider other ways to address data gaps.

B. Principles for Self-Regulation

9. Where the regulatory system makes use of Self-Regulatory Organizations (SROs) that exercise some direct oversight responsibility for their respective areas of competence, such SROs should be subject to the oversight of the Regulator and should observe standards of fairness and confidentiality when exercising powers and delegated responsibilities.

If there is any entity that operates or, in the future will operate, as a SRO for participants in the DeFi ecosystem, then such entity (whether or not incorporated) should be subject to the IOSCO SRO principle.

This Principle covers regulatory systems that make use of SROs that exercise some direct oversight responsibility for their respective area of competence. DeFi activities and participants, to the extent that they involve financial instruments, including securities, may already, depending on the jurisdiction, be subject to a jurisdiction's regulatory framework and perimeter, even if they are not currently operating in a manner compliant with the jurisdiction's regulatory framework.

The following are non-exclusive examples of types of DeFi activities that may be within the scope of activity covered by an SRO in certain jurisdictions, either currently or in the future, and to the extent not, these are the activities that could be the focus of addressing any gaps:

- Aggregators and Decentralized Exchanges (DEXs) involving crypto-assets that are financial instruments, including securities. These activities may be exchange, broker, dealer or adviser activity.
- Borrowing and lending activities involving crypto-assets that are financial instruments, including securities. These activities may be broker or dealer activity.
- Derivatives activities.

C. Principles for the Enforcement of Securities Regulation

10. The Regulator should have comprehensive inspection, investigation and surveillance powers.

11. The Regulator should have comprehensive enforcement powers.

12. The regulatory system should ensure an effective and credible use of inspection, investigation, surveillance and enforcement powers and implementation of an effective compliance program.

Regulators should have comprehensive inspection, investigation, surveillance and enforcement powers over DeFi activities subject to securities laws. The above Principles are to be interpreted broadly to ensure regulators have a variety of measures to detect, deter, enforce, sanction, redress and correct violations of securities laws.

The following are non-exclusive examples of types of DeFi activities that could involve securities activities subject to regulation in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators, DEXs and Automated market makers (AMMs);
- Trading/Lending/Borrowing/Derivative products and activities;
- The offer and sale of interests in DeFi products and services, including the offer and sale of tokens or other crypto-assets in exchange for the deposit of crypto-assets or borrowing of crypto-assets from any product;
- The offer and sale of governance tokens;
- Collective investment schemes, hedge funds and other private investment vehicles and investment pools;
- Providing investment advice about crypto-assets or crypto-asset trading activities, whether directly or indirectly;
- The activities of investors, collective investment schemes (retail/non-retail), hedge funds or other private investment vehicles, and others, in DeFi products, including in trading directly or through aggregators, DEXs, lending and borrowing activities.

D. Principles for Cooperation in Regulation

13. The Regulator should have authority to share both public and non-public information with domestic and foreign counterparts.

14. Regulators should establish information sharing mechanisms that set out when and how they will share both public and non-public information with their domestic and foreign counterparts.

15. The regulatory system should allow for assistance to be provided to foreign Regulators who need to make inquiries in the discharge of their functions and exercise of their powers.

As most DeFi activities occur cross-border, there is a need for regulators to cooperate as they evaluate the operation of such activities and participants in the DeFi ecosystem. The Principles for cooperation can serve as the basis for approaches to international cooperation and information sharing among regulators with respect to DeFi activities. Cooperation will allow regulators to minimize the likelihood that compliance programs, investigations and enforcement activities will be impeded by jurisdictional boundaries. Regulators should consider what cooperation tools are available for cross-border cooperation and information sharing.

E. Principles for Issuers

16. There should be full, accurate and timely disclosure of financial results, risk and other information which is material to investors' decisions.
17. Holders of securities in a company should be treated in a fair and equitable manner.
18. Accounting standards used by issuers to prepare financial statements should be of a high and internationally acceptable quality.

The Principles for issuers concern the information that issuers should disclose to investors when they invest in securities and on an ongoing basis. Full, timely and accurate disclosure of financial and non-financial information for DeFi projects would provide investors with information about the issuer, its management and ownership, the risks of investing in a particular security backed by a specific issuer and financial results or other information specific to the project.

Potential Issuers of Financial instruments, Including Securities: The following are non-exclusive examples of types of DeFi products, services, arrangements, and activities that could involve the issuance of financial instruments, including securities, in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators and DEXs, offering and selling their own crypto-assets, including governance tokens, LP tokens or other crypto-assets;
- Lending/borrowing products or services that offer and sell interests in their pools in exchange for crypto-assets. In these cases, market participants "deposit" crypto-assets into pools in exchange for an interest in the pool. These pool interests are represented by other crypto-assets or tokens that represent the depositor's *pro rata* value of the lending pool. The holder of the pool interest represented by the token can obtain value from it by trading it in secondary

markets, borrowing against it, or by presenting it to the pool for redemption of the crypto-asset deposited and all accrued *pro rata* income.

- Lending/borrowing products or services that offer and sell other crypto-assets, such as governance tokens, that may give the holder particular rights, whether to vote on aspects of the lending/borrowing product or service, or other economic interests in the lending/borrowing product or service.
- An AMM or other liquidity pool that offers and sells interests in the pool of crypto-assets that is the AMM. As with the borrowing and lending product tokens that are issued in exchange for crypto-assets deposited in the pools, AMM tokens are also redeemable by the holder for the crypto-asset plus the *pro rata* income from the pool.
- A developer, founder or promotor of DeFi protocols also may directly offer and sell crypto-assets, including in the form of governance tokens, or other crypto-assets. These offers and sales may occur at the initial funding of the protocols or may occur on an ongoing basis with sales of crypto-assets from the "treasury" of these protocols.
- Aggregators and DEXs also may be involved in offering and selling crypto-assets or tokens of other issuers, thereby participating in distributions of financial instruments, including securities. This may occur through the aggregator or DEX's operations or offerings through which creators or operators of DeFi protocols may distribute governance tokens or other crypto-assets, including crypto-assets that are placed in "treasury" for distribution.
- The issuance of derivatives, including derivatives/synthetics on traditional financial instruments, as well as the issuance by a cross-chain bridge, wrapping of a token, or in connection with liquid staking.

F. Principles for Auditors, Credit Rating Agencies, and Other Information Service Providers

19. Auditors should be subject to adequate levels of oversight.

20. Auditors should be independent of the issuing entity that they audit.

21. Audit standards should be of a high and internationally acceptable quality.

22. Credit rating agencies should be subject to adequate levels of oversight. The regulatory system should ensure that credit rating agencies whose ratings are used for regulatory purposes are subject to registration and ongoing supervision.

23. Other entities that offer investors analytical or evaluative services should be subject to oversight and regulation appropriate to the impact their activities have on the market or the degree to which the regulatory system relies on them.

DeFi activities and participants can involve auditors (whether due to laws and rules applicable to issuers or other participants providing audited financial statements or financial information or other types of auditor involvement), credit rating agencies (whether or not identified as such), and other information service providers (including index and pricing information providers).

The following are non-exclusive examples of types of DeFi activities to which the IOSCO Principles could apply, either currently or in the future:

- Any DeFi project providing audited financial information, including without limitation audited financial statements;
- Any DeFi project that provides any type of credit score may be viewed as a credit rating agency subject to principle 22. If a DeFi project posts or provides the credit ratings of an independent credit rating agency, then the principle applies to the independent credit rating agency.
- Some DeFi projects may offer analysis or evaluative services on their user interface or promote the result(s) of such services for a variety of reasons, including increasing investor engagement in the project or increasing investment in the protocol.
- Many DeFi projects rely on "oracles" to provide pricing information necessary to the operation of the projects. These oracles would likely be considered information service providers and subject to the IOSCO principle 23.[158] These oracles provide off-chain pricing information to smart contracts on an ongoing basis.

G. Principles for Collective Investment Schemes

24. ***The regulatory system should set standards for the eligibility, governance, organization and operational conduct of those who wish to market or operate a collective investment scheme.***

25. ***The regulatory system should provide for rules governing the legal form and structure of collective investment schemes and the segregation and protection of client assets.***

26. ***Regulation should require disclosure, as set forth under the Principles for issuers, which is necessary to evaluate the suitability of a collective investment scheme for a particular investor and the value of the investor's interest in the scheme.***

27. ***Regulation should ensure that there is a proper and disclosed basis for asset valuation and the pricing and the redemption of units in a collective investment scheme.***

28. ***Regulation should ensure that hedge funds and/or hedge funds managers/advisers are subject to appropriate oversight.***

[158] It is likely these oracles are also subject to IOSCO principles for financial benchmarks. *See* OICV-IOSCO, PRINCIPLES FOR FINANCIAL BENCHMARKS (July 2013), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD415.pdf.

Potential Collective Investment Schemes: DeFi products, services, arrangements, and activities may fall within the scope of collective investment schemes (retail/non-retail), hedge funds and other private investment vehicles. Further, DeFi activities and participants that involve operation, marketing, management and advising with respect to these funds may be subject to laws that apply to such activities in many jurisdictions. The following are non-exclusive examples of types of DeFi activities that could involve collective investment schemes (retail/non-retail), hedge funds or other private investment vehicles, and those who operate, market, manage and advise with respect to such funds in certain jurisdictions, or are similar to such activities and participants in others, either currently or in the future:

- Certain aggregators and DEXs may be creating collective investment schemes, hedge funds or other private investment vehicles through the use of AMM arrangements. For example, AMMs typically provide a means for participants to deposit two or more crypto-assets into a smart contract (or liquidity pool) and receive a crypto-asset representing the interest in the pool (and income therefrom). Market participants are then able to use aggregators, DEXs and other service providers to engage in trading activities with the pools. The pools may constitute collective investment schemes. While some of this activity may involve broker or dealer activity, the activity can also include the provision of investment advice. For example, some aggregators provide services that offer investment opportunities to users, such as by obtaining for users the best prices for crypto-assets.
- Lending/borrowing protocols also may involve collective investment schemes, funds and other private investment vehicles. Lending products are pools of crypto-assets deposited by holders in exchange for another token representing the interest in the pool. The lending product then enables other crypto-asset market participants to borrow the crypto-assets in exchange for interest payments. The pooled nature of these lending products may satisfy the definition of collective investment scheme in many jurisdictions. Operators of lending and borrowing protocols also may be viewed, depending on their structures, as investment advisors or sponsors of the collective investment scheme. Initially at least, these operators set the terms of the smart contract arrangements, such as the crypto-asset pairs available to trade, maintain the algorithm to update interest rates, set utilization rates, and address instances of default, including maintenance of a reserve factor.
- Some DeFi products may be structured and operate as hedge funds (or other private funds, or retail/non-retail collective investment schemes), depending on applicable laws. For example, vaults are a mechanism for retail investors to participate in allegedly on-chain hedge funds by deploying capital into single or multi-strategy pools run by smart contracts. The sale of the interests in these pools may be collective investment vehicles as they are offered to the public or, if limited to institutions, may be hedge funds. There are also hedge funds that invest or interact with DeFi activities, products and services and the IOSCO Standards applicable to hedge funds would apply to these hedge funds as well.

H. Principles for Market Intermediaries

29. Regulation should provide for minimum entry standards for market intermediaries.

30. There should be initial and ongoing capital and other prudential requirements for market intermediaries that reflect the risks that the intermediaries undertake.

31. Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, with the aim of protecting the interests of clients and their assets and ensuring proper management of risk, through which management of the intermediary accepts primary responsibility for these matters.

32. There should be procedures for dealing with the failure of a market intermediary in order to minimize damage and loss to investors and to contain systemic risk.

Potential Market Intermediaries: There are many DeFi products, services, arrangements, and activities that involve market intermediary participants or activities. This includes exchange, broker, dealer, investment advisor, custodian, clearing agency, transfer agent, and settlement activities, as well as providers of other services including proxy advisory and credit rating services. The following are non-exclusive examples of types of DeFi arrangements that could involve market intermediary activities in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators, DEXs, and other products and services facilitate the exchange of crypto-assets. DEXs can involve order book exchanges, through which DEXs are performing functions typically associated with exchanges. DEXs can also use AMMs, also known as liquidity pools, which provide liquidity for trading markets. AMMs may be seen to be acting as liquidity providers or market makers and thus engaging in buying and selling activities like brokers or dealers.
- Aggregators and DEXs also provide services to users to enable them to trade with multiple AMMs. These activities are akin to broker or dealer activity as well.
- The operation of lending/borrowing products also may involve broker or dealer activity, particularly to the extent that the crypto-assets in the pool are financial instruments, including securities, and the lending product is engaging in lending activities with respect to the crypto-assets that are financial instruments, including securities.
- Each of the AMMs and the lending products may also be engaging in custodial activities and acting as counterparties, due to the manner in which the products engage in holding customer crypto-assets and trading customer crypto-assets. Whether these products and protocols may be acting as custodians of crypto-assets may depend, in part, on how the crypto-assets are transferred to the smart contracts.
- Aggregators enable users to seek the most favorable terms across a variety of protocols. Aggregators allow users to source bids and offers, monitor prices and

execute transactions across multiple protocols and trading platforms from a single interface. These activities likely involve exchange, broker or dealer, or investment advisor activity, depending on the particular facts.

- Yield aggregators are platforms of investment opportunities which, depending on how they are structured, provide the functions of either or both a broker and/or an investment advisor. Some yield aggregators provide a type of asset management which has similar characteristics to automated investment or robo-advisory services.
- Portfolio aggregators' primary functionality gives investors visibility into their current positions and allows them to execute transactions from the aggregator's interface thus providing the functions of a broker or dealer.
- Aggregators specializing in governance protocols may centralize proposals and voting across various DAOs, providing recommendations on how to vote on certain proposals. In this capacity, these types of aggregators may be acting as proxy advisors, if voting is delegated to the protocol. Investors may exchange their voting right(s) for compensation in such arrangements.
- Promotors of DeFi products or services.

I. Principles for Secondary and Other Markets

33. The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.

34. There should be ongoing regulatory supervision of exchanges and trading systems which should aim to ensure that the integrity of trading is maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.

35. Regulation should promote transparency of trading.

36. Regulation should be designed to detect and deter manipulation and other unfair trading practices.

37. Regulation should aim to ensure the proper management of large exposures, default risk and market disruption.

Potential Exchange/Trading Systems: There are DeFi products, services, arrangements, and activities that could involve exchange and trading system activity. This includes exchange and over the counter activities, both in cash (spot) crypto-asset and derivatives markets. The following are non-exclusive examples of types of DeFi activities and participants that could involve exchange and trading system activity subject to regulation in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators and DEXs facilitate the exchange of crypto-assets. DEXs can involve order book exchanges, through which DEXs are performing functions typically associated with exchanges. DEXs can also use AMMs, also known as liquidity pools, that provide liquidity for trading markets.

- Aggregators and DEXs facilitate the trading of crypto-assets. These activities can involve exchange and trading system activities, and also may operate as an issuer or primary distribution mechanism for new tokens or crypto-assets.
- Aggregators and DEXs also may be acting as a market for derivatives. These kinds of derivatives trading activities include providing protection or selling protection against loss (similar to swaps activities), selling synthetic exposures based on the value of other assets (which could include securities), and engaging in *perpetual futures* trading activity.
- Certain lending/borrowing products may act as exchanges or trading systems depending on the particular structure.
- Many protocols enable automated, and often high-speed, trading, often by sophisticated, well-capitalized entities. Algorithmic trading is common in the DeFi space, and bots are employed to run various trading strategies or identify arbitrage opportunities. Oracles and bridges offer connectivity with off-chain data and between DeFi protocols.

J. Principles Relating to Clearing and Settlement

38. Securities settlement systems, central securities depositories, trade repositories and central counterparties should be subject to regulatory and supervisory requirements that are designed to ensure that they are fair, effective and efficient and that they reduce systemic risk.

Certain DeFi activities and participants involve clearing and settlement services and the existing IOSCO Principles for clearance and settlement, securities depositories, trade repositories, and central counterparties could apply.

Potential Clearing and Settlement Entities: The following are non-exclusive examples of types of DeFi activities and participants that could involve clearing and settlement activity subject to regulation in certain jurisdictions, or are similar to such activities in others, either currently or in the future:

- Aggregators and DEXs use DLT to transfer ownership of crypto-assets. Depending on the particular protocol, these crypto-assets may be held within an associated smart contract, nominally on behalf of the user of the protocol. Changes in ownership of crypto-assets within DEX and AMMs likely involve clearing and settlement activity.
- Lending/borrowing protocols, as with DEXs and AMMs, generally rely on associated smart contracts to hold crypto-assets and to effectuate transfers of crypto-assets in associated lending pools. Changes in ownership of crypto-assets lending/borrowing protocols likely involve clearing and settlement activity.
- The activities of certain types of aggregators may also be viewed as clearing and settlement activity. For example, yield aggregators are platforms of investment opportunities which, depending on how they are structured, can provide the functions of either or both a broker and/or an investment advisor while potentially acting as a central counterparty. These activities may also operate as

settlement systems, depositories, or central counterparties depending on their structure.

- Layer 1 blockchains could themselves be carrying out clearing and settlement activities.

ANNEX G – SUMMARY OF UPDATED SURVEY RESULTS AND OUTREACH

In November 2022, the IOSCO Fintech Task Force (FTF) Decentralized Finance Working Group (DeFi WG) issued a survey to members of the IOSCO FTF to obtain information regarding their current and planned regulatory approaches to DeFi and to inform the ongoing work of the DeFi WG (the *Survey*). The Survey requested information regarding, among other things: the regulatory treatment of DeFi within IOSCO member jurisdictions; DeFi activities, including challenges, risks, and trends, within IOSCO member jurisdictions; and regulatory engagement with DeFi market participants, stakeholders, academics, and researchers.

Regulatory Treatment of DeFi within IOSCO Member Jurisdictions

(a) Overview of the current regulatory treatment of DeFi activities

The Survey asked respondents to provide an overview of the current regulatory treatment of DeFi activities within their jurisdictions. All respondents stated that they do not have separate regulatory frameworks specifically dedicated to DeFi activities at this time. Most of the respondents noted that DeFi activities are currently viewed through the same regulatory frameworks that apply to other traditional financial products, services, and activities subject to financial regulation. Some respondents shared that they are currently reviewing their regulatory approaches in relation to DeFi and exploring ways to incorporate DeFi activities into those other regulatory schemes.

Some respondents noted that efforts are underway in their jurisdictions to create new regulatory frameworks specific to crypto-assets, and that those regulatory frameworks, while not specifically targeting DeFi, might in some instances apply to DeFi activities, e.g., where there are centralized issuers or service providers engaged in activity covered by those other regulatory frameworks. For example, while the EU's Market in Crypto Assets (MiCA) regulation does not specifically apply to DeFi, EU-based respondents indicated that MiCA could apply to DeFi where a regulated service/activity is performed/provided/controlled, directly or indirectly, by an identifiable natural/legal person and/or other undertakings, including when part of such activity or service is performed in a decentralized way.

Respondents acknowledged that it may sometimes be difficult to identify the centralized actors involved in DeFi arrangements, which could present enforcement challenges (discussed further below), but in general, those actors would be subject to these regulatory frameworks, as appropriate. Likewise, a purported lack of centralized authority or use of algorithmic rules/processes would not itself exempt such activities from existing financial regulations. Respondents also emphasized that a lot of DeFi activities appear to be "decentralized" in name only.

(b) Recent developments relating to regulatory treatment of DeFi

In addition to an overview of the current regulatory treatment of DeFi activities, the Survey sought information regarding any updates or developments relating to the regulatory treatment of DeFi activities, including, among other things, proposed legislation or regulations relating to DeFi, licensing or registrations relating to DeFi activities, supervisory or enforcement actions relating to DeFi, or other published guidance relating to DeFi.

(i) New or proposed legislation or regulations relating or specific to DeFi activities

The majority of respondents stated that their jurisdictions did not have any new or proposed legislation or regulations specific to DeFi activities, but reiterated that, in general and depending on the facts and circumstances, existing regulatory frameworks that apply to other traditional financial products, services, and activities could apply to DeFi. In addition, and as noted above, some respondents stated that there are currently efforts to create new regulatory frameworks specific to crypto-assets and crypto-asset service providers (e.g., MiCA in the EU), and that those frameworks could also apply to DeFi activities, where appropriate. For example, if a form of central authority/beneficiary is identified for a DeFi activity, then existing or upcoming rules might apply.

One respondent noted several ongoing initiatives in the EU relating to the development of a regulatory framework for DeFi, including an EU pilot project for the development of a technical solution to collect data on a blockchain, with a view to developing a supervisory approach for DeFi activities,[159] and the publication of a report by the EU Commission raising considerations for policymakers when thinking of an approach to the regulation of DeFi.[160]

(ii) Licensing or registrations relating to DeFi activities

Respondents generally stated that they do not have specific licensing or registration frameworks relating to DeFi activities, but that, consistent with the approach described above, existing licensing and registration frameworks could apply to certain DeFi activities and that the entities involved in those activities would generally be expected to comply with those existing frameworks. Most respondents stated, however, that there have not been any entities or persons licensed specifically in relation to DeFi activities in their jurisdictions.

(iii) Supervisory or enforcement actions relating to DeFi activities

[159] *See* https://commission.europa.eu/publications/commission-implementing-decision-financing-implementation-pilot-project-embedded-supervision_en ("The result of the pilot project should help to inform and prepare the application of new legislative instruments for decentralised finance.").

[160] *See* https://op.europa.eu/en/publication-detail/-/publication/f689e5b2-4f55-11ed-92ed-01aa75ed71a1/language-en/format-PDF/source-272370364.

Several respondents noted that they have brought public enforcement actions related to DeFi activities under their existing regulatory frameworks, including the U.S. SEC[161] and CFTC[162], Quebec AMF[163], and SC Malaysia[164]. Another respondent noted that after investigating a DeFi protocol offered in its jurisdiction, the respondent requested that the DeFi protocol stop such activity since it was considered a regulated activity (asset management).

Apart from the above, most respondents stated that there have not been supervisory or enforcement actions focusing on DeFi activities, but a few respondents noted that they are continuing to conduct regulatory activities, including investigations, relating to certain DeFi activities, and that despite the absence of public actions to date, DeFi activities may be subject to existing regulatory frameworks and, where appropriate, regulatory, supervisory or enforcement actions.

(iv) Guidance and other assistance for DeFi market participants

The Survey asked whether respondents have provided DeFi participants with any of the following: guidance related to regulatory requirements and the supervisory approach; warnings or statements over DeFi risks; assistance with licensing or registration; relaxation of, or waivers or exemptions from, certain regulatory requirements; product trial/testing frameworks; or trialing certain technologies with the authority.

A few respondents have published reports or guidance specific to DeFi. One respondent published guidance on DeFi that included a description of DeFi and associated risks and a discussion on the potential applicability of existing regulations to DeFi.[165] Another respondent published a report advising those who would use a Decentralized Autonomous Organization (DAO) or other distributed ledger or blockchain-enabled means for capital raising to take appropriate steps to ensure compliance with applicable securities laws.[166]

[161] *See* https://www.sec.gov/news/press-release/2021-145; https://www.sec.gov/news/press-release/2018-258.

[162] *See* https://www.cftc.gov/PressRoom/PressReleases/8478-22; https://www.cftc.gov/PressRoom/PressReleases/8590-22.

[163] *See* Décision - Autorité des marchés financiers c. Change Marsan inc. - 2021 QCTMF 43 (soquij.qc.ca);

Décision - Autorité des marchés financiers c. Hope - 2021 QCTMF 48 (soquij.qc.ca);

see also Décision - Autorité des marchés financiers c. CreUnite - 2018 QCTMF 8 (soquij.qc.ca)

(action taken against an issuer of crypto-assets that were qualified as securities (ICO), distributed (among other means) through a DEX).

[164] *See* https://www.sc.com.my/resources/media/media-release/sc-takes-enforcement-actions-on-binance-for-illegally-operating-in-malaysia.

[165] *See* BaFin - Decentralised finance (DeFi) and DAOs.

[166] *See* https://www.sec.gov/files/litigation/investreport/34-81207.pdf.

Another respondent published a primer explaining smart contract technology and related risks and challenges (as part of a broader body of guidance/information relating to the crypto-asset marketplace).[167] Other respondents noted that although they have not published any guidance specific to aspects of DeFi, they have published guidance relating to crypto-asset activity more generally, including regarding the applicability of their regulatory frameworks to crypto-asset activities and associated risks, which may also apply to DeFi.[168] A number of respondents have also issued public warnings relating to DeFi risks.[169]

In addition to public guidance, a number of respondents noted that they provide informal feedback to written and oral inquiries on matters involving crypto-assets and other financial technology, including those that may involve DeFi, often through an "innovation hub" or the equivalent. These respondents stated that they may engage with entrepreneurs and market participants and assist them, to varying degrees, with questions relating to the applicability of relevant regulatory requirements, including licensing and compliance issues. One respondent also noted that their innovation hub has a specific intake form for inquiries related to DeFi. Several respondents also noted the availability of a "sandbox" or other type of product trial/testing framework in their jurisdiction relating to FinTech more broadly, as well as some development activity relating to DeFi specifically.[170]

Finally, one EU-based respondent noted that it engages with market participants as part of its regulatory horizon scanning and has gathered positive feedback regarding the proposed regulation of DeFi. That respondent noted that market participants have expressed an interest for a coordinated international approach to DeFi regulation, in light of the cross-border nature of DeFi activities.

DeFi Activities within IOSCO Member Jurisdictions

(a) DeFi activities

[167] *See* https://www.cftc.gov/PressRoom/PressReleases/7847-18.

[168] *See, e.g.,* https://www.cftc.gov/PressRoom/PressReleases/8336-20; https://asic.gov.au/regulatory-resources/digital-transformation/crypto-assets/; https://www.osc.ca/en/securities-law/instruments-rules-policies/2/21-329/joint-canadian-securities-administratorsinvestment-industry-regulatory-organization-canada-staff; https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf; https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-regulatory-framework-for-virtual-asset-portfolios-managers; https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=18EC77; https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=22EC10.

[169] *See* https://www.moneysense.gov.sg/articles/2022/10/defi_what-you-need-to-know;

https://www.esma.europa.eu/sites/default/files/library/esa_2022_15_joint_esas_warning_on_crypto-assets.pdf

(focusing on crypto-assets generally but mentioning DeFi).

[170] *See, e.g.,* https://www.mas.gov.sg/news/media-releases/2022/first-industry-pilot-for-digital-asset-and-decentralised-finance-goes-live.

The Survey sought information regarding the following DeFi activities or business models observed in IOSCO member jurisdictions: DAOs; stablecoin offerings and use; credit/lending; decentralized exchanges/trading; liquidity or investment-type pooling; automated market marking; mining/staking/pooling; yield farming; insurance/risk management; asset management; and derivative and other synthetic product offerings. Several respondents said that they have observed all of the above activities within their jurisdiction. Most of the respondents said that they have observed some, but not all, of the activities. Some respondents noted that they have not observed any of the aforementioned DeFi activities within their jurisdictions.

Several respondents noted that based on publicly available sources, it appears that DeFi activities may originate from and/or be available in their jurisdictions, but due to the pseudonymous or anonymous nature of blockchains, it is difficult to identify exactly where the activity is and whether it does involve persons in their jurisdictions. It appears that most DeFi activities are open to participation by all persons, including retail investors, across borders.

One respondent noted that they have evaluated the types of persons and entities who participate in DeFi. Based on that respondent's initial observations, including anecdotal information, there are a variety of persons and entities that have a current or future interest in DeFi, including: (i) brokers, dealers and investment advisers; (ii) token issuers, including through the use of smart contracts; (iii) token distributors; (iv) investors (including institutions and venture capital firms); and (v) developers.

One respondent also noted that due to the lack of transparency in the DeFi "market", there is a lack of data about the level of activity of each of the participants at any particular level of DeFi structure, platform, or layer. The ability to evaluate each type of current DeFi product, service, arrangement and activity is therefore limited. However, based on a review of some of the more active DeFi platforms, that respondent has observed that there often are multiple components and a combination of different types of activities. Thus, while that respondent has observed market activity in each of the types of DeFi activities listed in the Survey, such activity may not be engaged in on a standalone basis, but instead may be part of a larger arrangement. For example, a single entity may create a decentralized trading platform, offer what is termed a *governance token*, may create a derivative product, and may use a crypto-asset termed a *stablecoin*. In addition to the lack of transparency in, and the constantly evolving nature of, DeFi structures, in some cases the project's public statements may not fully or accurately describe how the structure actually operates and what is being offered.

Respondents reported observing the following specific types of DeFi activities in their jurisdictions:

- Stablecoin offerings and use. A number of respondents said that they are aware of various types of stablecoins that are in circulation. These stablecoins have varying characteristics. For example, the stablecoin may be *pegged* or *linked* in some way to a reference asset, which could be fiat currencies, another crypto-asset, a real asset, or some combination of assets. Certain stablecoins claim to provide holders a 1:1 direct redemption right against an issuer or reserve of assets while others do not.[171] In addition to the use of stablecoins on crypto-asset trading platforms, participants in DeFi structures may use stablecoins as one side of the trade in DeFi transactions. An example would be the use in purchase and sale transactions with AMMs that often allow for stablecoins to be deposited into smart contracts formed as liquidity pools. In these transactions, a combination of stablecoin and some other crypto-asset is deposited through a smart contract into a pool of crypto-assets. Market participants could exchange one token for the other at an exchange rate set by an AMM that typically uses a mathematical formula driven by the relative proportion of the two types of crypto-assets in the pool to determine the exchange rate. Stablecoins also are often used in DeFi structures as collateral deposited into a protocol to support lending and borrowing activities. A number of DeFi structures also issue their own stablecoins.

- Credit/Lending. Respondents have observed arrangements that appear to provide for a lending structure in return for a payment. In these structures, crypto-asset trading platforms, smart contracts, or other market participants create a credit/lending pool. They borrow crypto-assets from clients or other market participants and lend these crypto-assets to other market participants in return for a fee. In a number of the smart contract structures, participants may deposit one type of crypto-asset as collateral and in return, borrow a different crypto-asset from the credit/lending pool. To date, many credit/lending pools (including smart contracts establishing such pools) or lending platforms require, as a condition to participation, that borrowers provide an amount of crypto-asset collateral well in excess of the value of the crypto-assets borrowed.

- Decentralized Exchanges/Trading. Respondents have observed entities that claim to have set up DEXs that purportedly allow for the trading of crypto-assets (referred to as *tokens*) between parties, including tokens that appear to be securities, by both retail and institutional investors. Initially, these DEXs used an order book structure and used the ox protocol as the underlying technology. This enabled any person to list orders, but trading was relatively slow and expensive with gas fees of $50-100 [per transaction]. Although *order book* DEXes now face competition from the AMMs discussed below, there are innovations, including DEXes that claim to offer high-speed, on-chain order books.

- Liquidity or Investment-type Pooling / Automated Market Making. Respondents have observed arrangements involving the creation, through smart contracts, of *liquidity pools* or AMMs. AMMs generally hold two types of crypto-assets and offer users the ability to trade one of the crypto-assets in the pool for the other at a price

[171] One respondent referenced the IOSCO stablecoin report, FSB stablecoin reports, and US PWG stablecoin reports for further information.

determined by a c*onstant product* function. Users that deposit tokens to the AMM, providing liquidity, often receive another crypto-asset called a *liquidity provider token*, that may entitle the holder to a portion of fees generated through the use of the AMM. AMM protocols can also issue governance token. Traders can transact with the pools directly or through entities that provide *routers* that seek to find the best prices across many AMMs. Many of these smart contracts and structures are copies of or based on code written originally by Uniswap. The liquidity/AMM pools appear to be funded (or *capitalized*) by market participants who seek a return based on the trading profits of the AMM. Sometimes, participants share in fees generated by the AMM/liquidity pool as part of the trading activities, often through liquidity provider tokens, governance tokens and also through secondary trading on crypto-asset trading platforms of the liquidity provider tokens and governance tokens.

- <u>Governance Tokens.</u> Governance tokens are issued, directly or indirectly, by an entity establishing a particular platform or system and are issued in different manners and for different purposes. For example, in some cases governance tokens are issued to persons participating in transactions on an entity's blockchain or through their platform or system or upon presentation of another crypto-asset issued through their platform or system. Others may be issued as additional consideration for equity and other investments in an entity's platform or system, and these governance tokens could be issued as rewards to developers or employees. These tokens may be associated with certain voting rights over certain aspects of a DeFi protocol.
- <u>Yield Farming / Asset Management.</u> Respondents have observed arrangements that involve what is called *yield farming*. Generally, yield farming involves a series of transactions, involving borrowing and lending crypto-assets, in which the party attempts to start purchases and sales with one asset and through a *daisy-chain* engages in a series of purchases and sales that result in a profit on each one. For example, this can involve a person holding *Token A* who lends that to a *lending/credit* pool to get *Token B*, and then they deposit Token B in a liquidity pool and get *Token C*. This transaction enables potential returns at each level. One respondent has observed yield farming arrangements that offer to manage borrowing and lending of client or market participants (including retail investors) crypto-assets using multiple lending pools and multiple platforms. For example, some yield farming entities offer to take crypto-assets from another market participant (including retail investors) in return for a promise of a return, and then will deploy these assets in various DeFi structures and arrangements. The types of uses may involve collateral for crypto-asset loans to the yield farming operator, or as deposits into AMM/liquidity pools.

- <u>Insurance/Risk Management.</u> Respondents have observed arrangements that appear to incorporate DeFi components in order to pay a counterparty for losses related to DeFi transactions. For example, people sell digital tokens that purport to entitle the holders to receive money if an event occurs. Often, these arrangements require off-chain assessments and inputs, provided by humans and/or oracles. One respondent has seen examples of insurance coverage that would be triggered by oracles that identify: (1) a bug in a smart contract; (2) customer losses due to theft from a crypto-asset trading platform that holds customer crypto-assets; or (3) a flight being delayed or cancelled. One respondent noted that while these protocols state that they are insurance products, it does not appear that the entities offering the insurance are regulated insurance companies.

- <u>Derivative & other Synthetic Product offerings.</u> Respondents have observed DeFi structures that offer digital tokens, through smart contract pools, that are marketed as providing synthetic exposures to other financial instruments, including securities and commodities. For example, some entities claim that they have issued crypto-assets and created systems (through their smart contracts) that will cause the value of the crypto-asset to rise, and fall based on the performance of a referenced asset or index, such as a stock or commodity. It is not clear what type of derivative exposures these asserted synthetic crypto-asset structures provide, such as whether they provide total return exposure (payments based on the performance of the linked asset, including any payments on such assets, such as dividends or payments on common stock) or event exposures (payments based on the occurrence of an event).

<u>Other services or activities.</u> Respondents have also observed the following:

- One respondent has observed DeFi offerings of what appear to be crypto-asset notes (borrowing by an entity and lending by a market participant) that are stated to have a return based on an investment in physical assets. There may be elements of liquidity or creditor pools involved in these structures. These types of crypto-asset structures also could involve other types of investment activities and offer profit sharing based on the performance of the investments.
- One respondent has observed DeFi prediction markets that allow *bets* to be made through the creation of smart contract pools. These include structures that offer the ability for a user to create an event contract that will pay off based on future events, for example the outcome of an election or economic events. The participants creating that event contract will receive a fee and for purchasers of the crypto-asset representing the contract exposure, they may trade the crypto-asset during the life of the contract and, at the end of the contract, the holder winning the bet will be paid through a smart contract.
- In addition to the various categories of DeFi activity, several respondents noted that they have observed an increasing role by centralized intermediaries (whether platforms or other types of FinTech companies) facilitating retail consumer access to DeFi protocols, which may indicate increasing interlinkages between DeFi and CeFi.

(b) Challenges in regulating or attempting to regulate DeFi activities

Respondents highlighted a number of challenges in regulating or attempting to regulate DeFi activities, including the following:

- <u>Determining how existing regulatory frameworks should be applied to DeFi activities.</u> Respondents noted that determining whether DeFi activities, including new/emerging types of services, fall within existing regulatory frameworks can be challenging. Respondents attributed these challenges to a few different factors. One respondent noted that the inner workings of DeFi protocols may not be very transparent or easy to understand, such that determining how existing regulations should be applied can be difficult and time consuming. And although some DeFi activities are similar in risks and economic substance as existing regulated activities, they may not fall so neatly within existing legal definitions because of the way they are structured or offered, e.g., using smart contracts. In addition, there may be challenges in determining which transactions and participants and which entities facilitating the transactions are subject to existing regulations. This challenge implicates questions such as which activities of software developers of smart contracts would require registration as a regulated entity, and how decentralization of a project potentially complicates application of regulatory requirements.

- <u>Lack of, or difficulty identifying, central actors to whom existing regulation should apply.</u> Respondents noted that there may be limitations in exercising existing regulatory and enforcement authorities due to the potential absence of, or inability to identify, a central actor who can be held accountable. Given the alleged lack of central authority (i.e., due to distributed governance and/or distributed code development and maintenance), it can be challenging to attribute the provision of DeFi services, and responsibility for compliance, to a responsible party or appropriate stakeholders (e.g., who is responsible for operating or implementing changes to a given protocol). Respondents indicated that this uncertainty on who should be held accountable for DeFi activities is exacerbated given that smart contracts run autonomously to provide services and that governance may be decentralized to varying degrees and involve the use of governance tokens and / or DAOs. Thus, even when an authority determines that a certain DeFi activity falls within its regulatory perimeter, there may not be identifiable persons or legal entities to hold responsible or engage on an ongoing basis in relation to complying with the applicable regulations. One respondent noted that "true DeFi" (if it exists), where all actors would be unknown, might create insurmountable challenges in terms of who should be in charge of ensuring compliance with the regulatory requirements. Business continuity, market integrity, and investor protection concerns might also be exacerbated in such circumstances.

- <u>Lack of information.</u> Related to the above, respondents noted a general lack of transparency and/or reliable information relating to DeFi activities, including a lack of data on the size and scope of DeFi activities in jurisdictions, which leads not only to difficulties in applying existing regulations (as noted above), but also to other issues, including challenges in supervising such activities and legal and evidentiary challenges when trying to enforce regulations relating to those activities. Respondents noted that the lack of data and transparency on the developers and operators behind the DeFi protocols, i.e., pseudonymity, makes it hard to monitor DeFi activities or gather information and evidence against bad actors. This presents particular challenges for enforcement agencies to prove a case, as it may be difficult to identify stakeholders and to determine the "victims." Related to that, respondents noted that there is a need to build up crypto-asset enforcement capabilities, as record-keeping is done on public blockchains and within smart contracts. Respondents noted that the prevailing pseudonymity in DeFi also makes it very challenging to assess financial risks such as credit, liquidity and leverage risk, as well as the interconnectedness with the traditional financial system and other segments of crypto-asset markets (e.g., CeFi) and also with third-party technology providers.

- Technological complexity of DeFi. Respondents also cited difficulties in understanding the details of DeFi activities, which are technical and complex, noting that available descriptions of DeFi activities (where they exist) are often basic and insufficient for a comprehensive legal assessment. In certain cases the ability to read and understand smart contracts may be required, as many protocols publish only rudimentary information and descriptions. Related to this, respondents noted a lack of resources and know-how to monitor and interpret these activities, and that existing information gathering tools and methods may not be effective in analyzing and monitoring DeFi activity, especially given the pseudonymous nature of the parties and information. Respondents noted that even if data is available on public blockchains, the capabilities to aggregate, read, and analyze such that may be limited. The quick pace of innovation exacerbates this and other challenges, making it difficult for regulators to keep up with DeFi market developments.

- Cross-border issues. Respondents noted that the owners and operators of DeFi products and services may be based in multiple jurisdictions and providing their offerings on a cross-border basis, such that regulatory cooperation is essential. In the absence of such cooperation, it would be difficult to identify the applicable jurisdictions and pursue enforcement actions against responsible parties located abroad. In addition, given the borderless nature of DeFi activities, there may not always be a regulatory nexus to assert jurisdiction over the activities. For instance, where investors in one country access a DeFi platform on a permissionless blockchain and trade digital tokens, the regulators may have challenges enforcing that jurisdiction's regulations against the platform where there is no presence or solicitation in the country. Respondents indicated that the borderless nature of DeFi activities calls for a globally coordinated approach to regulation, including better international cooperation among regulators to strengthen surveillance, develop consistent regulations, and enhance information gathering.

- <u>Consumer protection challenges.</u> Respondents noted that although the code that facilitates DeFi transactions is often open source, most consumers do not take the time or have the expertise to review the code and instead rely on other factors when deciding to trust that transactions will process as expected. There have been numerous instances over the years of the economic incentives and the smart contract security of DeFi protocols being exploited and leading to individual or network-wide economic loss. Accordingly, respondents noted concerns with consumer protection/lack of awareness of risk related to such transactions.

(c) Developments or trends in DeFi market

Respondents were asked to describe developments or trends in the DeFi market that require particular attention from a regulatory and supervisory perspective. Some of the respondents reiterated some of the same aforementioned challenges in regulating or attempting to regulate DeFi as issues that require attention from regulators. In addition, respondents noted the below developments or trends:

- The speculation, embedded leverage, re-hypothecation of collateral, and interconnectedness that exist within the DeFi ecosystem (see, e.g., the Terra's UST/Luna collapse), and the lack of data / transparency on such interconnections;
- The financial stability implications arising from the interconnectedness within the DeFi and crypto-asset ecosystems, as well as between DeFi and TradFi;
- The emergence of centralized intermediaries, which purport to make it easier for retail clients to overcome technical barriers to access DeFi;
- As an example of some of the above, crypto-asset service providers offering attractive, and likely unsustainable, yields for customers that hold crypto-assets with them, where the returns are generated through staking and lending activities (where the service providers participate in unregulated DeFi protocols using customers' crypto-assets);
- Sources of vulnerability specific to DeFi allowing attack vectors, such as governance attacks (manipulation of DeFi protocol design parameters to steal liquidity from deposits in the protocol) or flash loans (transactions allowing users to borrow an asset without providing any upfront collateral);
- Market integrity issues within the DeFi ecosystem, e.g., price oracle manipulation, front-running transactions, and other types of market manipulative activities; and
- Investor protection concerns arising from the increasing number and scale of successful cyber attacks, as well as frauds and scams, involving DeFi protocols.

(d) Organizational structure to responding to DeFi, development of tools and techniques, and internal expertise related to DeFi

The Survey sought information regarding who within respondents' organizations take the lead in responding to DeFi. Most of the respondents noted that DeFi issues or developments are monitored and assessed in the first instance by a centralized team, whether it be an innovation or FinTech-focused hub, department, unit, or coordination team, and then referred to other subject matter experts within the organization as appropriate (e.g., for licensing/registration, enforcement, policy development, etc.). The respondents indicated that these teams generally take the lead in responding to DeFi related questions, tracking DeFi market developments and reviewing academic and other source materials. A few respondents stated that they are also in contact with other subject matter experts, such as those in academia and industry, and have attended trainings to develop internal expertise related to DeFi, blockchain analytics, smart contract audits, and other relevant topics.

The survey responses indicate that respondents generally have not developed their own tools or techniques to obtain data on the level of DeFi activities and models. One respondent noted, however, that in addition to its innovation group, the respondent has a dedicated supervisory technology office, which has been conducting research to gain a better understanding of areas like crypto, blockchain, DeFi and web3.0. That group is exploring relevant tools, data sources and information sources that can contribute to the understanding, and engaging external researchers, industry players, and DeFi experts to understand the latest technology, products, trends and risks. They also support knowledge sharing with other departments and organize courses to improve the organization's knowledge in crypto/DeFi area.

(e) Risks to and protection of participants, stakeholders, and markets

The Survey asked respondents to describe risks that they have observed to participants, stakeholders, and markets related to DeFi. A few of the respondents reiterated some of the same challenges discussed above relating to the regulation of DeFi, including issues relating to the applicability and effectiveness of existing laws for DeFi, the anonymous and pseudonymous nature of DeFi activities, a lack of understanding and information relating to DeFi activities, the cross-border nature of DeFi activities, and the extremely fast pace development.

In addition to those challenges, one respondent noted that in general, the risks that arise in traditional securities markets, such as counterparty risk, liquidity risk, and risk of fraud and loss of investor funds, may be implicated in the DeFi market as well. In addition, to the extent that DeFi markets and DeFi market participants, such as intermediaries, fail to comply with applicable laws and regulations, investors and other market participants will generally lack investor protections and other protections, and are subject to greater risk that they may be defrauded, with limited ability for redress, either through private means or government enforcement. In addition, to the extent that DeFi market participants engage in activity that is subject to regulation, the failure to comply with regulatory requirements puts investors and connected markets, including securities markets, at risk.

Respondents also noted other risks for participants, stakeholders, and markets related to DeFi, including:

- Governance risks, including opaque governance structures, concentration of governance tokens, and differences between perceived and actual levels of decentralization

- Lack of prudential measures for certain DeFi services, which could result in investor losses
- Technology and cybersecurity risks and vulnerabilities, including code hacks or key theft, *smart contract risk* (i.e., the technical level of security of the smart contract code), coding errors within the smart contracts or underlying protocols, and other technical malfunctions
- Inadequate technology and cybersecurity controls and business continuity planning and disaster recovery procedures
- Lack of information on and availability of identifiable responsible operators in case of malfunctions, legal disputes, etc.
- Inadequate disclosures to / lack of awareness by investors of, among other things, how DeFi protocols operate, the underlying risks of a DeFi service, product or activity, and other information, such as the business model, services offered, related parties, and conflicts of interest of DeFi market participants
- Market manipulation and fraud, including code or oracle exploits, rug pulls, protocol back doors, and fraudulent platforms
- *Wrapping complexity*, where derivatives of tokens are repeatedly created, giving rise to new risks and interconnections between different protocols
- AML risks, including the movement of hacked / stolen funds and the potential lack of legal responsibility for DeFi protocols due to automation
- Reliance on third-party information providers or validators, such as oracles and other outside data sources, could potentially increase risks if those third-party sources produce faulty information—either because it is inaccurate or it has been manipulated

The Survey also asked whether jurisdictions have evaluated opportunities for DeFi arrangements to comply with regulations that aim to ensure protection of market participants, stakeholders, and markets. In general, respondents underscored that their innovation/FinTech hubs welcome discussions with DeFi market actors about product development (and in some cases, have engaged in such discussions), and that the general expectation would be for DeFi activities to comply with existing/planned regulatory frameworks, as appropriate. One respondent noted that given the permissionless nature of most DeFi arrangements, these arrangements would likely encounter difficulties in attempting to comply with certain regulatory requirements. Along those same lines, another respondent stated that a key requirement to ensure compliance with existing laws and regulations would likely be the presence of an accountable natural/legal person identifiable as responsible for the performance of the relevant activities.

One respondent noted that a registered firm in its jurisdiction plans to offer a private fund that will engage in DeFi activities (including staking, lending. and participation in liquidity pools). Terms and conditions were imposed on the fund manager to address the risks of those activities, and the terms and conditions are publicly available.[172]

(f) Fraud, code exploits and operational risks related to DeFi

The Survey sought information from respondents regarding publicly reported details of fraud, code exploits and operational risks related to DeFi activity in their jurisdictions. Respondents acknowledged public reports of frauds, code exploits, and operational risks involving DeFi, with one respondent noting that public reports indicate that fraud is common in DeFi.[173] Apart from the enforcement actions discussed above, however, most respondents did not identify any specific instances or details of fraud, code exploits, or operational risks relating to DeFi in their jurisdictions. Several respondents explained that for most publicly reported cases, it is unclear which jurisdiction(s) are impacted as DeFi platforms typically operate cross-border/globally.

Regulatory Engagement

The Survey sought information regarding which jurisdictions have been engaging directly with DeFi market participants and stakeholders, as well as academics, researchers, or others aside from DeFi market participants or stakeholders, to evaluate DeFi and monitor market trends. A number of respondents noted that they have, through their innovation or FinTech hubs, engaged with participants involved in the DeFi space in an effort to better understand its structure, scope, and implications. This includes developers, investors and other interested parties, including academics, researchers, and other non-industry members of the public, to varying extents, ranging from engagement at industry events to bilateral meetings.

Respondents gave a number of examples of such engagement, including:

- One respondent held a DeFi workshop with participants from the financial industry, industry associations, business consultants, and law firms. That respondent has also discussed DeFi projects with supervised entities and new projects on a bilateral basis.
- One respondent is carrying out a joint research project with a prominent business school with the goal of measuring interconnections between crypto-assets and traditional financial assets and identifying the primary main transmission channels, the output of which will be contagion risk indicators that will be published in a report.

[172] *See* https://info.securities-administrators.ca/nrsmobile/nrssearch.aspx (search for "AQN Asset Management LTD" under "Firm," click on the name of the firm underlined in blue, and then scroll under Ontario, Terms & Condition 1. "Click for Details").

[173] *See, e.g.*, Theodore Claypoole, *Ubiquitous and Creative Fraud is Regular Feature of Defi*, NAT'L L.REV., Apr. 27, 2022, available at https://www.natlawreview.com/article/ubiquitous-and-creative-fraud-regular-feature-defi; CHAINALYSIS, *supra* note 21; ELLIPTIC, THE STATE OF CROSS-CHAIN CRIME (Oct. 2022), available at https://www.elliptic.co/resources/state-of-cross-chain-crime-report.

- One respondent noted that its jurisdiction has established a committee, composed of lawyers, academics, and other qualified individuals, that is currently conducting work in relation to the DeFi space.
- One respondent noted that it has established a FinTech advisory group, composed of experts from academia, consulting firms, the central bank, and industry, which has been regularly providing input to on FinTech matters, including DeFi, for several years.
- Several respondents noted that they have engaged some subject matter experts, such as blockchain analytics companies and law firms, to better understand DeFi and DeFi market trends, including the different types of DeFi and how they are structured.
- Several respondents noted that they also include academic and other source materials in their horizon scanning of developments in the DeFi space.

Respondents noted several challenges that they have encountered in engaging with DeFi market participants. One of the challenges noted by multiple respondents is the decentralized nature of DeFi activities, which appears to result in a lack of legal entities or offices and anonymity. Further, some respondents commented that it could be difficult to fully understand and keep track of the DeFi market due to its complex structures, business models, products, and technologies, which are constantly evolving. Another challenge that was noted (and also discussed above) is the difficulty in finding reliable sources of data, e.g., on Total Value Locked, the number of DeFi protocols, and DeFi volumes, to enable such engagement.