Final Report with Policy Recommendations for Decentralized Finance (DeFi)

THE BOARD

OF THE

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR/14/2023	**December 2023**

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 Report to finalize IOSCO's policy recommendations to address market integrity and investor protection issues in decentralized finance (DeFi).[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.

[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 Report are focused on DeFi. IOSCO has separately published recommendations related to Crypto and Digital Asset Markets more generally. *See* IOSCO, POLICY RECOMMENDATIONS FOR CRYPTO AND DIGITAL ASSET MARKETS FINAL REPORT (Nov. 2023), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf .

Table of Contents

EXECUTIVE SUMMARY

DeFi commonly refers to financial products, services, activities, and arrangements that use distributed ledger or blockchain technologies (DLT), including self-executing code referred to as smart contracts. DeFi aims to operate in a disintermediated and decentralized manner, eliminating some traditional financial intermediaries and centralized institutions, and 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. IOSCO encourages responsible innovation that benefits investors and the markets, and 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 report sets forth nine policy recommendations 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 in November 2023. The two sets of IOSCO recommendations have been developed in accordance with IOSCO's Crypto-Asset Roadmap (Roadmap) published in July 2022.[5] Concurrently with the publication of this report, IOSCO is publishing an "Umbrella Note" to explain the interoperability between the two sets of recommendations.

The 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, activities, and arrangements by applying IOSCO's widely accepted global standards for securities markets regulation.

---

3 DeFi is a term used in industry and broader discussions. It may 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, activity, or arrangement decentralized. This report notes that certain DeFi arrangements are in fact providing financial products, services, and activities 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 FINAL REPORT (Nov. 2023), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.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 prioritizing 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 markets, given the cross-border nature of these 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 regulation/regulatory outcome."

The 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, provide their services, and engage in activities across multiple jurisdictions.

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

SECTION I. INTRODUCTION TO THIS 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 regulation/regulatory outcome" approach to financial markets, regardless of the technology that may be used to offer or provide financial products and services or to engage in financial activities. 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 and provided, what financial activities are being engaged in, who are offering or providing those products and services or engaging in those activities, and to whom regulatory obligations may apply. This report is intended to assist IOSCO members in reaching that understanding based on their own analyses. As the 2022 Report notes, applicable regulatory frameworks apply to DeFi products, services, activities, and arrangements, notwithstanding characterizations or assertions of decentralization by persons or

---

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 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.

entities controlling or sufficiently influencing such products, services, activities, and arrangements.

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 and provided.
- ***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, activities, and arrangements.

Acknowledging the definitional and interpretive jurisdictional differences that currently exist, IOSCO has developed the 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 common DeFi products, services, activities, and arrangements, 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) provides a brief overview of the state of DeFi, highlighting developments since the 2022 Report. A more detailed overview is contained in the annexes to the consultation report that preceded this report ("DeFi Consultation Report"). This is 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, activities, and arrangements.

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

Section IV (Summary of Feedback) contains a summary of public feedback received during the consultation process, along with IOSCO's responses.

SECTION II. STATE OF THE DEFI MARKET

The 2022 Report provided a comprehensive overview of the DeFi market, including DeFi products, services, activities, and arrangements, based on information available at the time of its publication. This section provides: (A) an overview of DeFi's common products, services, and activities; (B) a brief 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, Services, and Activities Using DLT

Persons and entities are currently offering financial products, providing financial services, and engaging in financial activities that, at least in part, utilize code deployed on public permissionless DLT-based platforms. These products, services, and activities 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 financial products and services referred to as DeFi mimic or resemble those of traditional financial markets. Moreover, the code that implements a DeFi protocol is created, deployed, operated, and maintained by humans. Nor are DeFi products, services, or activities currently offered, provided, or engaged in without human involvement. Further, the smart contracts operating on a blockchain typically are only one component of the product, service, or activity. For the most part, the products, services, and activities referred to as DeFi are offered, provided, and engaged in by persons or entities using traditional components and infrastructures as well as smart contracts and blockchains.[8]

The 2022 Report details various common DeFi products offered, services provided, and activities engaged in. The DLT-based components associated with these products, services, and activities are commonly referred to as DeFi protocols. Common 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, and this report provides an abbreviated description below for ease of reference. With respect to each of these protocols, certain parameters typically can be set and/or altered by person(s) or entity/entities, such as a developer, project team, or through certain governance decision-making, such as by voting by holders of tokens in a Decentralized Autonomous Organization (DAO).

[8] *See* 2022 Report, *supra* note 6, at 7-8.

Decentralized Exchange (DEX)[9]

Persons or entities create a DEX to provide 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 person or entity 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 interested in buying or selling a particular crypto-asset at a certain price (makers) communicate their order to the person or entity, 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 person or entity operating the DEX may never have control, through the DEX or otherwise, of the users' crypto-assets and may serve as a relayer of information that is necessary for the trade to be executed and settled on the blockchain. The person or entity controlling the DEX 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). Persons or entities who provide 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 is then 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 ratio of assets within the pool. AMM-based DEXs are substantially dependent on arbitrage traders, typically employing bots, which are programmed to buy or sell crypto-assets for profit until the liquidity pool price converges with the average market price.

---

9 *Id.* at 14-15.

Lending/Borrowing[10]

Persons and entities create lending/borrowing protocols to provide a service that allows holders of crypto-assets, often stablecoins,[11] to earn a fixed or variable return on those assets by depositing them in a smart contract (or lending pool) that simultaneously allows other participants to borrow those assets. Depositors typically receive a different crypto-asset, 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. 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, providers of the lending and borrowing protocol typically seek 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]

Persons and entities create aggregators to provide services that 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. Aggregator services 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

---

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 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 6, at 15-16.

best trade terms available. Providers of aggregator services 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 enables a particular financial product, service, or activity. 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). As with traditional enterprises, there are persons or entities that engage in various operations, initially and on an ongoing basis. Those persons and entities at the enterprise level are described in the 2022 Report as the *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 operate the enterprise (such as founders, developers, and foundations); those investing in the enterprise (such as investors); those involved in the ongoing activities in controlling and managing the enterprise, including 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 enterprise (such as service providers, oracles, bridges, and miners/validators). It could be that the enterprise itself offers a financial product, provides a financial service, or engages in a financial activity. It could also be that others associated in some way with the enterprise do so. In any event, each of the stakeholders in any particular DeFi 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 at the enterprise level.[13]

In analyzing DeFi arrangements and activities, 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 way they operate does not materially differ from that of traditional financial markets.[14] Upon close examination, these stakeholders and their roles, and the organizational, technological, and communication mechanisms they use, tend to mimic or resemble those that regulators are used to seeing in traditional finance. Therefore, the choices of persons, for example, to organize as a 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-

---

[13] The *Big Picture* diagram in the 2022 Report illustrates a common scenario describing arrangements and activities in DeFi. It can serve as a useful guide for regulators as they analyze any particular DeFi arrangement or activity at the enterprise level.

[14] *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.").

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 offer or provide financial products and services and engage in financial activities should be subject to applicable laws.

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

Fuelled by the use of stablecoins and an influx of participants through centralized crypto-asset platform on-ramps, the combined Total Value Locked (TVL)[15] 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. As of the end of November 2023, the combined TVL in the DeFi ecosystem amounts to approximately $47 billion.[16]

Significant 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.[17] For example, in 2022, the algorithmic stablecoin[18] 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. 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. 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 steps to freeze their BUSD

---

15 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.

16 *See* DEFILLAMA, https://defillama.com.

17 *See* FSB DeFi Report, *supra* note 13, at 18.

18 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.

markets. 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. This, in turn, caused disruptions in the DeFi markets. These significant events and their respective impacts in DeFi are explained in greater detail in ANNEX A to the DeFi Consultation 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.[19] Also, in the wake of these events, the DeFi market appears to have become more concentrated, with reports indicating, for example, that the top four DEXs hold about 54% of the total market share of all DEXs.[20]

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. ANNEX B to the DeFi Consultation Report explores in greater depth 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 2021. Of that $3.1 billion, 64% was attributable to attacks on cross-chain bridges.[21] Another blockchain analytics firm reported that nine of the ten largest attacks occurred against DeFi projects.[22] Reports

---

19 *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.

20 *See* DeFi Is Becoming Less Competitive a Year After FTX's Collapse Battered Crypto - Bloomberg, Nov. 16, 2023 (citing data from industry sources).

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

22 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-

indicate that hacker groups associated with North Korea are among the most prolific.[23] Reportedly, North Korean-linked hackers have stolen $1.1 billion in crypto-assets through hacks of DeFi protocols.[24]

Recent reports also assert that DeFi protocols increasingly are used for money laundering and other illicit uses and misconduct.[25] 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.[26] 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.[27]

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 with respect to DeFi. Proponents of DeFi often claim that blockchain ecosystems are 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.

2023#:~:text=TRM%20Labs%20data%20indicates%20that%20cryptocurrency%20wallets%20that%20receive%20victim,large%20transnational%20organized%20crime%20groups.

23 *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).

24 CHAINALYSIS, *supra* note 23, at 60.

25 *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. *See also* IOSCO, RETAIL MARKET CONDUCT TASK FORCE FINAL REPORT (Mar. 2023), available at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD730.pdf; Solidus 2023 Crypto Market Manipulation Report - Part One, Insider Trading, available at https://www.soliduslabs.com/reports/2023-crypto-market-manipulation-reports; Solidus 2023 Crypto Market Manipulation Report - Part Two, Wash Trading, available at https://www.soliduslabs.com/reports/2023-crypto-market-manipulation-report.

26 CHAINALYSIS, *supra* note 23.

27 FATF, *supra* note 25, 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.").

There exist several challenges to the accessibility and interpretability of relevant data, including:[28]

- ***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 persons or entities controlling a smart contract or protocol.[29] 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.[30] 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.[31] 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 (e.g., liquidity pair smart contract), persons or entities controlling a smart contract or protocol 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

---

28 The Financial Stability Board has also discussed data challenges in a recent report. *See* FSB DeFi Report, *supra* note 13; *see also* Report of FSA's Joint Research on Analyzing Decentralized Financial System Using On-Chain And Off-Chain Data (June 2023) QUNIE Corporation, available at https://www.fsa.go.jp/policy/bgin/Research_Paper_QUNIE_en.pdf (identifying data sets relevant to DeFi).

29 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.

30 For example, the US Securities and Exchange Commission recently filed a case alleging that, among other things, the promotors of a particular DeFi arrangement 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.pdfhttps://www.sec.gov/litigation/complaints/2023/comp-pr2023-32.pdf.

31 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.

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 to the DeFi Consultation Report.

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, certain types of 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).[32] The FSB DeFi Report describes a panoply of risks, such as operational fragilities, liquidity and maturity mismatches, leverage, and 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

[32] FSB DeFi Report, *supra* note 13.

regulation.[33] 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.[34] 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.[35] 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.[36]

The risk discussion in ANNEX E to the DeFi Consultation Report 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, which generally involve governance of persons and entities controlling/influencing a DeFi product, service, or activity, 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 persons or entities controlling/influencing financial products, services, and activities, 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.

---

33 *Id.* at 16.

34 *Id.* at 23.

35 *Id.*

36 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 to the DeFi Consultation Report; public source research and outreach to industry, academic and researchers; and feedback received from public consultation. The recommendations and guidance describe how regulators can analyze DeFi products, services, activities, and arrangements, and are intended to support authorities in jurisdictions seeking to apply IOSCO's Standards to DeFi through existing regulatory frameworks, as well as those 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, activities, and arrangements across the IOSCO Principles for Securities Regulation, which includes a mapping of certain DeFi products, services, activities, and arrangements to those found in traditional finance. A complete mapping is found in ANNEX F to the DeFi Consultation Report. 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, activities, and arrangements.

IOSCO is issuing these policy recommendations to help IOSCO members apply relevant existing IOSCO Standards through their own regulatory frameworks, as appropriate, to DeFi products, services, activities, and arrangements 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, in the manner 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.[37]

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, services, activities, and arrangements behave like substitutes for securities or other regulated financial instruments and activities involving such securities and financial instruments, and (2) investors have substituted securities or other financial instruments and investment activities with DeFi products, services, activities, and arrangements.[38]

In the crypto-asset markets, along a spectrum of arrangements, persons and entities typically offer financial products, provide financial services, and engage in financial activities that substantially mirror those in traditional financial markets. 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 regulation/regulatory outcome."

---

37 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.

38 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.

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 offer and provide DeFi products and services and engage in DeFi activities attempt to arrange and distribute their operations outside of traditional organizational forms. While persons or entities may not be using traditional organizational forms, in most cases, there are persons or entities who are controlling or have sufficient influence over the financial product, service, or activity being offered, provided, or engaged in. It is possible that, in certain instances, it may be more challenging to identify the specific persons or entities engaged in offering the product, providing the service, or engaging in the activity 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 analyses.

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 financial product, service, activity, and its risks, regulators can apply the same regulation or aim to achieve the same regulatory outcome.

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

A regulator should analyze DeFi products, services, activities, and arrangements, occurring or located within its jurisdiction, with a view to applying its Existing Framework or New Framework, as appropriate, to the offer of financial products, the provision of financial services, and the engagement in financial activities (or to products, services, and activities that behave like, or have been substituted by investors for, financial products, services, and activities), in accordance with the principle of "same activity, same risk, same regulation/regulatory outcome." To do so, a regulator should aim to achieve a holistic and comprehensive understanding of such DeFi products, services, activities, and arrangements. A regulator should assess what technological knowledge, data, and tools the regulator needs to understand, and analyze DeFi products, services, activities, and arrangements, to inform regulatory responses.

Guidance

Understanding DeFi products, services, activities, and arrangements 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, activities, and arrangements; 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, and traditional market participants, play.

In assessing whether a particular DeFi arrangement, or any part of it, falls within a regulator's jurisdictional remit, ideally the regulator should aim to gain a holistic understanding of the particular arrangement 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 activities conducted by 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 market participants. The *Big Picture* diagram in the 2022 Report identifies and describes 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, and how the arrangement is controlled or influenced. 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, whether there are financial products being offered, financial services being provided, or financial activities being conducted, by the arrangement itself, or by any persons or entities associated in some way with the arrangement. Many of the products, services, and activities in DeFi mirror, and in some cases overlap with, products, services, and activities found in markets for traditional securities and other regulated financial instruments. A potential starting point for this analysis is to map particular products, services, or activities of the DeFi arrangement to those

in traditional finance. 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 and in ANNEX F to the DeFi Consultation Report 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, activities, and arrangements. This type of analysis requires understanding the relevant technologies in the *tech stack* associated with the DeFi arrangement.[39] 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 an associated smart contract or protocol, including through the inclusion or ordering of transactions (i.e., 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 and protocols 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, activities, and arrangements. 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, activities, and arrangements 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 is often pseudonymous or anonymous and can be difficult to decipher without the required tools and expertise. Off-chain data, such as that available from crypto-asset trading platforms, typically is not audited or otherwise verified. ANNEX C to the DeFi Consultation Report provides a detailed analysis of data gaps and challenges in DeFi.

---

[39] *See* 2022 Report, *supra* note 6, at 3-4.

Effective market surveillance requires greater oversight of on-chain and off-chain data across platforms. Regulators should make efforts to improve cross-market data transparency and regulatory reporting, supported by high-quality and comparable data, similar to the data that is now available in traditional financial markets. As this is currently a continuing challenge in crypto-asset markets, regulators should consider how to address this issue, which may include market-led solutions and/or regulatory requirements placed on Responsible Persons to report relevant data. In addition, IOSCO intends to (1) conduct work amongst its members going forward to promote the development of data standards that could help to improve the availability, and improved access to better and more homogenized international data sets, and alongside this (2) encourage its members to develop appropriate solutions within their jurisdictions to help further these objectives.

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

Recommendation 2 – Identify Responsible Persons

A regulator should aim to identify the persons and entities of a purported DeFi arrangement that could be subject to its applicable regulatory framework (Responsible Person(s)).[40] These Responsible Person(s) include those exercising control or sufficient influence over a financial product offered, financial service provided, or financial activity engaged in (or over products, services, and activities that behave like, or have been substituted by investors for, financial products, services, and activities) by the DeFi arrangement.

Guidance

A Responsible Person(s) generally is a person(s) or entity/entities that offers, provides, engages in, or facilitates the offering, provision, or engagement in, financial products, services, or activities. Responsible Person(s) includes those that exercise or can exercise control or sufficient influence over a particular financial product, service, or activity. The person(s) or entity/entities who is a Responsible Person(s) may, for example, offer or sell a financial instrument or other investment product, or provide the services of, or engage in activities of an exchange, broker, dealer, or investment advisor, or those of a collective investment scheme, hedge fund or other investment vehicle, among other activities.

Some industry participants have asserted that if something is decentralized, it is not, or cannot be, regulated. Most commonly, the term decentralization in DeFi refers to the state of a particular governance or decision-making mechanism, often enabled by the use of governance/voting tokens

[40] Responsible person(s) is meant broadly, to encompass, for example, natural persons, groups of persons, entities and organizations, whether formally or informally constituted. There may be more than one Responsible person for any particular DeFi product, service, or activity.

and DAOs.[41] However, regardless of a governance structure or how "decentralized" the decision-making is, there is usually a Responsible Person(s) that controls, or sufficiently influences, the offer of products, provision of services, or engagement in activities. In conducting its analysis, a regulator should carefully examine any claim that an arrangement is purportedly decentralized to the point that no persons or entities are responsible for a financial product, service, or activity, and seek to identify any Responsible Persons within its applicable regulatory framework.

The determination of whether a person(s) or entity/entities is a Responsible Person(s) for regulatory purposes is based on whether, in fact, they control or sufficiently influence the offer of financial products, provision of financial services, or engagement in financial activities, regardless of the form they use to organize and regardless how "decentralized" that organization is.[42] Who or what a Responsible Person(s) is in any given case will be based on specific facts and circumstances. In some cases, that control or sufficient influence may reside with a single person or small group of persons. In other cases, a larger group of persons can have control or sufficient influence. For example, a group of persons or an entity or entities using governance/voting rights or organized as a DAO may be acting collectively to direct themselves or others to make changes to a financial product, service, or activity. In some cases, more than one person or entity may be a Responsible Person.

Also, whether the Responsible Person(s) is organized in a legal corporate form or some other form should not be determinative of whether the actual financial product, service, or activity at issue, or those controlling or sufficiently influencing it, is or should be subject to regulation. For example, while a DAO may be decentralized in terms of its governance, the focus is on whether the DAO itself is offering a product, providing a service, or engaging in an activity subject to regulation. If it is, the DAO, as a person(s) or entity, would be the Responsible Person with regard to the product

---

[41] DAOs are often governed through the use of "governance" or "voting" tokens, which can be issued in connection with the participation in certain products, services, or activities. These governance tokens represent interests in the entity controlling the product, service, or activity, such as a DAO, giving the holders the right to participate in the entity management and activities. In some cases, these governance tokens represent an economic interest in the entity and its revenue from the DeFi protocols, products, services, and activities the entity controls.

[42] *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 ("[Creators, 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.").

being offered, service being provided, or activity being engaged in. The lack of control by a single person in a DAO should not negate the existence of a regulatory touchpoint vis-a-vis a Responsible Person. This is no different than in traditional finance, where general partnerships or joint ventures can be and are subject to regulation, even though the management and operation of the partnership or venture is shared among the participants.

In some cases, those who have control or sufficient influence over decision-making for a DeFi arrangement at the enterprise level (see Recommendation 1 above) will be Responsible Persons with respect to a particular financial product, service, or activity if, for example, the enterprise itself is offering the product, providing the service, or engaging in the activity. In other cases, only a part of the enterprise may be doing so and, in that case, that part will have Responsible Person(s). Again, this is no different than in traditional finance, where regulatory obligations in some cases reside with a parent company and, in other cases, with subsidiaries or affiliates.

In determining who or what has control or sufficient influence, a regulator can consider, for example, those with design and maintenance control; financial and economic control; and formal and legal control, among other things. 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 or activities, a regulator should evaluate all the facts and circumstances, including: (a) the roles of persons and entities and how those persons and entities interact with each other and how those roles and relationships may evolve over time; (b) the ability of persons and entities, such as developers or foundations or DAOs, to control or influence a product, service, or activity offered, provided, or engaged in, including through actions that would impact a smart contract, protocol, or any particular product, service, or activity offered, provided, or engaged in, whether by setting or adjusting parameters, controlling user funds or assets, altering transactions, or controlling access or information with respect to the product, service or activity, entering into agreements that impact the product, service, or activity, or exercising some other control or influence; (c) whether there are others exercising control or influence over the product, service, or activity, such as venture capital firms, large investors, or governance/voting token holders or voters; and (d) how a regulator might apply regulatory oversight over these persons or entities.[43] Indicia of control or influence can include, for example, ownership interest; significant financial

[43] *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.").

interest; significant voting rights; management of or the ability to impact the operations of the product, service, or activity; the ability to set permissions or access rights for users of a protocol, or to otherwise impact the rights of other users of the protocol; control over a smart contract that holds user assets; and the ability to enter into legal agreements for the protocol or enterprise. What constitutes control may also depend on the relevant regulations in a jurisdiction.

When considering persons and entities that may be Responsible Persons, it is important to note that code currently used in DeFi arrangements is not self-implementing. Human involvement typically is necessary to build and deploy code, and to effectuate governance decisions to change code, i.e., to translate and implement proposals to make changes to an arrangement's protocol, smart contracts or other code into usable code. So those making and voting on governance proposals often must rely on others with technical control and skill (i.e., administrative access and requisite technical capability) to implement governance decisions. To the extent it is possible that code could also be designed to be 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 to the DeFi Consultation Report gives a detailed analysis of how governance currently operates in DeFi and can be a useful starting point for analyzing governance mechanisms.

Typically, the following person(s) or entity/entities are involved in some way with a DeFi arrangement, and each could be examined to determine their status as a Responsible Person(s), depending on the facts and circumstances:

- founders and developers;
- 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 smart contracts and/or protocol to some degree);
- those who have or take on the responsibility of maintaining/updating a protocol or other aspects of the arrangement, such as access rights;
- those with access to material information about the arrangement 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.

Again, the determination of Responsible Person(s) depends on who or what is controlling or has sufficient influence over the offer of a financial product, the provision of a financial service, or financial activity engaged in. Once a regulator identifies a Responsible Person(s) with respect to the offer of a financial product, the provision of a financial service, or financial activity engaged in, the Responsible Person(s) should be subject to Existing Frameworks or New Frameworks, as appropriate, in accordance with the principle of "same activity, same risk, same regulation/regulatory outcome."

Further, regardless of who a Responsible Person is for the purpose of complying with regulatory obligations in any particular jurisdiction, there may be other persons and entities liable for misconduct, fraud, or other violations of law, aside from non-compliance with regulatory obligations, such as an employee of a broker who commits insider trading or engages in market manipulation. In evaluating liability of particular persons or entities for misconduct, the regulator should also consider all laws that may govern, including those governing personal liability, controlling person liability, aiding, abetting and causing liability, and the like.

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, activities, and arrangements 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, activities, and arrangements 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, activities, and arrangements. 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, activities, and arrangements that may fall within the scope of securities or other financial instrument laws. The mapping in ANNEX F to the DeFi Consultation Report details how the IOSCO Standards apply generally to DeFi products, services, activities, and arrangements.

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, activities, and arrangements 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 an issuer, the risks and costs of investing in or using a particular DeFi product or service, relevant governance structures, 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 or related activities 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. Finally, a regulator should also assess how their regulatory framework takes into account the varying degrees of sophistication of investors in DeFi.
- **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, activity, and arrangement 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.[44]

As regulators consider to what extent IOSCO Standards and regulatory frameworks within their jurisdictions might apply to particular DeFi products, services, activities, and arrangements, 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, Activities, and Arrangements, and Activities to Traditional Finance

The following mapping may be a helpful starting point for determining what DeFi products, services, activities, and arrangements could fall within the remit of any particular jurisdiction. For a more detailed explanation of how common typologies in DeFi mimic or resemble traditional finance, see the 2022 Report[45] and ANNEX F to the DeFi Consultation Report.

Potential Issuances of Financial Instruments, Including Securities: The following are non-exclusive examples of types of DeFi products, services, activities, and arrangements 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:

---

44 *See* CDA Report, *supra* note 4.

45 2022 Report, *supra* note 6.

- Aggregators and DEXs that issue 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 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, activities, and arrangements 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 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 aggregators' 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, activities, and arrangements 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, activities, and arrangements 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 regulation/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.[46]

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 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 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 Responsible Person 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 Responsible Person may take advantage of their control or influence over a product, service, or activity to promote proposals or initiatives that inure to their benefit financially. Conflicts could also arise if the Responsible Person is engaged in multiple activities in a vertically integrated matter, either themselves or with affiliated parties. For example, the Responsible Person 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.

---

[46] 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.").

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.

Because of the complexities and opacities in DeFi arrangements, investors may be unaware that such conflicts may exist. However, conflicts of interest can exist independently of the level of decentralization of an arrangement. 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 of interest, therefore exacerbating risks. Also, it is important to note that various activities within a DeFi arrangement are controlled or performed by persons or entities, notwithstanding that aspects of the arrangement may be automated.

It may be unclear to a user the role and capacity in which a Responsible Person of a product or service is acting at all times. Concerns around conflicts of interest are further heightened if the Responsible Person of the DeFi product or service is in a fiduciary or similar relationship with a user. This could be the case if, for example, the Responsible Person has control over an investor's or user's funds or assets, is providing investment advice to the investor or user, or otherwise has assumed a fiduciary role with respect to the investor or 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.

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 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.

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 the DeFi Consultation 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.

A regulator should require 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.

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 Responsible Person 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 Responsible Person 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.

Depending upon the particular product or service, a Responsible Person of DeFi products and services can rely significantly upon underlying blockchain networks for computation and settlement, and for oracles and cross-chain bridges for interoperability of the product, service, or activity 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 Responsible Person 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.[47]

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.

Maximal Extractable Value (MEV)

Among other things, MEV can refer to the exploitation of mempool data[48] 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 a mempool and/or inserting other transactions that are added to a block to be appended to a blockchain. Notably, in certain traditional market contexts, the ability to order, insert, and otherwise control transactions enables conduct that may be considered manipulative and unlawful in a particular jurisdiction.[49] In any event, this activity in DeFi markets can result in transactions failing to achieve execution on the terms expected by transaction participants. Such activity could take the form of typical MEV exploits, the most common involving what has been referred to by participants as "front-running," "back-running," and "sandwich attacks" (see ANNEX B to the DeFi Consultation Report):

- "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 ordering transactions in 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.[50]
- "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.

---

47 *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.

48 Mempools consist of transactions that are waiting to be processed by the blockchain's miners/validators.

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

50 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.

- 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.

Regulators should evaluate the ability of a Responsible Person to identify and disclose, and, to the extent practicable, manage and mitigate 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 also be conflicts of interest that would need to be identified and addressed with respect to the Responsible Person of a product or service 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. If those conflicts exist, they should be assessed in accordance with Recommendations 4 and 6 as well.

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 to the DeFi Consultation Report. For example, both oracles and cross-chain bridges have been prone to significant hacks and exploits. One industry report calculates that DeFi protocols lost more than $400 million in 41 separate oracle manipulation attacks in 2022 (see ANNEX E to the DeFi Consultation Report), and that 64% of the $3.1 billion stolen from DeFi protocols in 2022 was attributable to cross-chain bridges[51] (see ANNEX B to the DeFi Consultation Report).

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

[51] CHAINALYSIS, *supra* note 23, at 58.

structures that may not be suited to addressing technological and operational risks in a timely and effective manner. Regulators should seek to require Responsible Person 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.

Smart Contract Audits

Certain DeFi arrangements may claim to have obtained a so-called smart contract "audit" in connection with their DeFi product, service, or activity. Generally, a smart contract audit is a term used by participants to describe a voluntary method for offering assurances about a DeFi arrangement's code. Participants may be offering these types of assessments to provide investors or users assurances in a particular DeFi arrangement's legitimacy, functionality, governance mechanisms, cybersecurity, and other features. However, while a smart contract audit may be useful in identifying potential vulnerabilities in specific smart contracts, protocols, or blockchain networks, these types of services in practice may not provide meaningful assurances to investors and users.

For example, despite claims to the contrary, a typical smart contract audit may only verify whether the code implements a particular design, but it may not give any meaningful assurances as to whether, for example, the design is fit for a particular purpose, can be misused by the designer or others, functions in the way it purports to function, or is governed in the way it purports to be governed.

A financial statement audit, by comparison, is required by many jurisdictions in connection with certain financial activities; for example, many jurisdictions require public companies to have their financial statements audited by independent auditors according to established auditing standards.[52] Unlike financial statement auditing, DeFi code assessments are voluntary, and are not subject to internationally-adopted standards. Code assessors typically operate according to the engagement contract the code assessor has executed with the DeFi arrangement. As a result, the methodology used by various smart contract assessors can differ from one to another.[53]

---

[52] *See, e.g.*, The Value of High Quality Audits and the Importance of Funding an Independent Multi-stakeholder International Standard-setting Structure (iosco.org).
Professional accountants serve a critical role in the global financial reporting ecosystem, both in the preparation of a company's financial information in accordance with the applicable financial reporting framework and in the performance of auditing and assurance services over a company's financial and non-financial information. Financial statement users, including investors, other capital providers, regulators, and stock exchanges, are the direct beneficiaries of high-quality work of professional accountants. The quality of their work is facilitated by high quality, internationally-adopted standards, particularly:
- Ethics standards for professional accountants, including auditor independence requirements issued by the International Ethics Standards Board for Accountants (IESBA); and
- Auditing, assurance and quality control standards issued by the International Auditing and Assurance Standards Board (IAASB).

[53] *See, e.g.*, How We Audit: A Comprehensive Guide to CertiK's Auditing Methodology - Blog - Web3 Security Leaderboard; How To Audit A Smart Contract: A Deep Dive Into Hacken's Process - Hacken.

Moreover, with smart contract audits, there are no specific audit requirements for the engagement or the information reported, allowing an entity employing such an assessment the full discretion to manage the terms of the assessment. For example:

- the extent and frequency of the code assessments performed;
- the determination of what code and other information is subject to the assessment;
- the type and level of assurance provided (for example, reasonable, limited, or no assurance) and the standards applied;
- the type and expertise of assurance provider engaged (i.e., affiliated or independent); and
- whether the results are made public, including the extent and format of the information shared.

In addressing the lack of uniformity and reliability in code assessments, regulators, as appropriate and consistent with their respective jurisdictional mandates, could consider whether to encourage or require the use of independent code assessments that adhere to applicable standards, including those that may be developed, relating to a DeFi arrangement, in order to promote investor and market protection in the DeFi markets.

Recommendation 6 – Require Clear, Accurate, and Comprehensive Disclosures

In applying Existing Frameworks or New Frameworks, a regulator should seek to require 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, activities, and arrangements 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, services, activities, or arrangements 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, activities, and arrangements can result in significant information asymmetries, where users and investors are not fully apprised of the nature of the products, services, activities, and arrangements 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 Responsible Persons, as appropriate, 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 be clear, concise, non-technical, and accurate as to the key features and risks related to the products, service, and activities at issue. They 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. Disclosures should also include a description of the governance and lines of responsibility and accountability within an offeror or provider of the product or service, including identifying key persons and the roles they play in the offer or provision of the product or service as well as, as appropriate, related parties and outside service providers. Information in marketing and promotional communications provided to investors should be consistent with such disclosures, and all such promotions and marketing of DeFi products and services should accurately and sufficiently disclose the product and service provided as well as the associated risks in a manner that is fair, clear, and not misleading. A regulator should also assess how disclosures take into account the varying degrees of sophistication of potential investors, including retail investors.

Regulators should require 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 activities, and arrangements, including their Responsible Persons, 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 regulation/regulatory outcome," DeFi products, services, activities, and arrangements, and their Responsible Persons, 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 or others 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 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, activities, and arrangements, should have the ability to cooperate and share information with regulators and relevant authorities in other jurisdictions with respect to such products, services, activities, and arrangements. 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

DeFi products, services, activities, and arrangements often are based in multiple jurisdictions and/or DeFi products and services are offered/provided on a cross-border basis. Those with control or sufficient influence over the product or service can be geographically dispersed across a number of jurisdictions. At the same time, there is often a lack of transparency regarding the Responsible Person, including their 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 products and services 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 are controlled by an entity or group that employs a distributed governance structure or that various

[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 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.

actors involved in the arrangement or activity are geographically dispersed. Some Responsible Persons may choose an organizational structure such as a 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.

Recognizing the cross-border nature of DeFi products, services, activities, and arrangements, regulators should have the ability to cooperate and share information to assist one another to fulfill their respective mandates relating to such products, services, activities, and arrangements. 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 and activities (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 participants 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 participants, 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 participant is engaged, and other relevant features of the DeFi activities of the participant, including the size and scope of the DeFi products and services offered by the participant and the participant'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 participants engaged in DeFi activities, including to provide other regulators with access to the books and records of those participants, 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 regulation/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.

---

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.

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

When analyzing DeFi products, services, activities, and arrangements, 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 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, activities, and arrangements.

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 to the DeFi Consultation Report. 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.

---

[57] CDA Report, *supra* note 4.

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]

Entity	**Potential Relationship to DeFi (Non-Exhaustive)**
Issuer of financial instruments, including securities	Issue crypto-assets; 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]

---

58 *See also* FSB DeFi Report, *supra* note 13, at 25-26; BIS, THE CRYPTO ECOSYSTEM: KEY ELEMENTS AND RISKS 15 (July 2023), available at https://www.bis.org/publ/othp72.pdf ("[Risks along the bank-crypto nexus extend beyond (direct and indirect) exposures because of the potential negative externalities 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. SUMMARY OF FEEDBACK AND IOSCO RESPONSES

On 7 September 2023, IOSCO consulted on a set of 9 proposed policy recommendations. The feedback period closed on 19 October 2023, with a total of 45 responses received from a range of stakeholders falling into these broad categories:

1. Industry Association (20)
2. Blockchain Governance (6)
3. Legal Advisor (5)
4. CASP (2)
5. Regulatory Authorities (2)
6. Traditional Finance Entity (2)
7. Blockchain Analytics and Intelligence (2)
8. Think Tank (2)
9. Natural Person (2)
10. Payments Provider (1)
11. International Organizations (1)

The IOSCO Board is grateful for the responses and took them into consideration when preparing the Final Report with Policy Recommendations for Decentralized Finance (DeFi) (Final Report). The rest of this section summarizes the replies received on the consultation questions.

Policy Recommendations for Decentralized Finance

IOSCO requested feedback on 10 questions, which are listed below:

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.

   Do you find the interoperability between this report and the IOSCO CDA Report to be an effective overall framework? If not, please explain.

The feedback received can be summarized in eight categories:

1. **Definition of DeFi, Taxonomy, Governance mechanism**

Summary of feedback

Numerous respondents emphasized the need for additional clarity in the descriptions of DeFi products, services, activities, and arrangements outlined in the Report, particularly focusing on specific characteristics of DeFi protocols and arrangements, and asked IOSCO to provide a global definition and taxonomy for DeFi. Several respondents described the definition of DeFi as excessively broad, requesting more particularity. These respondents noted the difficulty in evaluating the scope of the Report, citing the possibility of varying interpretations and unintended consequences.

Several respondents were of the view that additional clarity on the distinction between DeFi protocols and other DeFi arrangements was necessary, drawing distinctions between technology that allows peer-to-peer connectivity and applications designed to provide end-users with an interface to engage in transactions involving financial instruments. These respondents caution that DeFi regulation should not bring assets or activities that are outside the scope of financial market regulation into the scope of that regulation because of their use of DLT or other related technologies.

Multiple respondents expressed the view that certain topics were not fully described in the Report. One respondent sought additional detailed commentary on non-fungible tokens (NFTs), while another requested deeper analysis on a variety of topics including decentralized stablecoins, liquid staking platforms, and AMMs.

Numerous respondents commented on the Report's assessment of governance mechanisms. Many of the comments received were generally supportive of the Report's assessment of governance. However, several of the respondents requested further guidance regarding what constitutes governance and/or control vis-a-vis DeFi activities and their governance mechanisms. A few of these respondents also proposed definitions (e.g., taxonomies) and guidance of their own regarding their views of what constitutes governance.

Some respondents expressed the view that decentralization occurs on a continuum and that the Report did not adequately acknowledge that governance mechanisms vary on this continuum and therefore should be evaluated accordingly depending upon where on the continuum a particular DeFi activity fell. These respondents were generally of the view that there is a need to clarify the level of decentralization, to differentiate between activities that are "decentralized in name only" and those that are "truly decentralized".

Additional points of emphasis included the need for cooperation with the stakeholders, a nuanced understanding of decentralization, and tailored regulations that accurately reflect the complexities of the DeFi ecosystem. There was also a call to appropriately

distinguish Centralized Finance (CeFi) and DeFi to avoid potential overlap and confusion.

IOSCO's response

While IOSCO acknowledges the wide breadth of DeFi products, services, activities, and arrangements contemplated in the Report, developments over a relatively short timeframe demonstrate their emergent and evolving structures and complexities. A constantly expanding variety of offerings to potential end users, and the continuing urgency for investor and market protections in the DeFi ecosystem, necessitate the broad scope contemplated in the Report.

Recommendations have been developed considering the definitional and interpretive jurisdictional differences, rather than attempting to develop a one-size fits all prescriptive taxonomy. The Report already 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.

IOSCO's approach focuses on the economic substance of novel activities and the applicability of standards to these activities, and IOSCO does not regulate by prescribing taxonomies to its individual members. This allows regulatory approaches to adapt and apply to new or novel financial activities involving securities or other regulated financial instruments. The recommendations are designed to be principles-based and provide high-level guidance so that regulators can take into account their respective domestic landscape, mandates, and applicable regulatory frameworks. Also, it is not for IOSCO to opine on jurisdictional legal classification matters, which is the responsibility of our individual members. Therefore, some suggestions related to the development of a globally consistent definition and taxonomy for DeFi cannot be considered. That said, when applying or developing regimes to cover the governance of DeFi activities, IOSCO members should arrive at consistent regulatory outcomes with those expected in traditional finance.

As for governance mechanisms, sufficient detail is already set out in the report regarding the wide-ranging nature of varying governance mechanisms related to DeFi activities. As the Report notes, given the similar economic functions and activities of DeFi and traditional financial markets, many existing international policies, standards, and jurisdictional regulatory frameworks are applicable to those DeFi activities and those mechanisms that govern them.

We therefore consider that no changes to the approach consulted are necessary. However, Recommendation 1 has been updated to clarify that, in analysing DeFi, regulators should focus on the offer of financial products, the provision of financial services, and the engagement in financial activities (or to products, services, and activities that behave

like, or have been substituted by investors for, financial products, services, and activities).

The report has been changed to add clarifying language.

2. Achieve Common Standards of Regulatory Outcomes

Summary of feedback

While many respondents agreed that DeFi should be regulated in a manner consistent with "same activity, same risk, same regulation/regulatory outcome", many also disagreed that DeFi posed the same risks as TradFi given that DeFi activities are conducted via automated smart contracts without the need for intermediaries. Some respondents are of the opinion that transposing regulations for TradFi activities to DeFi activities does not always achieve the same regulatory outcome and that DeFi poses novel risks that existing regulatory frameworks were not designed to address.

Multiple respondents expressed the view that the uniqueness of DeFi activities and governance structures calls for bespoke regulation separate from existing regulatory regimes and that the Report's assessment of these mechanisms did not adequately take what they perceive as a need for a new regulatory regime into account.

They argued that DeFi risks cannot be addressed by a one-size-fits-all approach and suggested considering a fit-to-purpose regulatory framework focused on achieving the same outcome, instead of focusing on applying the exact same regulatory framework.

A few respondents stressed that the approach of applying "same activities, same risk, same regulation/regulatory outcome" regulation to DeFi activities would be inappropriate for DeFi activities whose governance is "truly decentralized", analogizing to open internet standards or "public good" infrastructure.

IOSCO Response

IOSCO agrees that there are some novel operational and technological risks posed by DeFi arrangements and activities, including those stemming from the use of DLT and smart contracts.

This is already taken into account under Recommendation 3, which states that regulators should consider whether existing requirements need to be tailored or adapted to address DeFi-specific features and risks. Recommendation 5 also calls for the operational and technological risks unique to DeFi to be addressed.

As the Report notes, given the similar economic functions and activities of DeFi and traditional financial markets, many existing international policies, standards, and

jurisdictional regulatory frameworks are applicable to those DeFi activities and those mechanisms that govern them.

IOSCO is not developing a one-size-fits-all approach as suggested by some feedback received. Regulatory authorities may opt to take different approaches taking into account the specificities of their jurisdictional legal framework.

That said, when applying or developing regimes to regulate DeFi activities, above all, IOSCO members should arrive at consistent regulatory outcomes with those expected in traditional finance. The DeFi recommendations are suitably high-level and cater to different types of regulatory frameworks while delivering investor protection and market integrity.

No change.

3. Responsible Persons: Scope and Guidance

Summary of feedback

Many respondents commented that the scope of Responsible Persons was too broad. Specifically, a number of them called for clearer definition of what constitutes "control" and "sufficient influence" so as to aid the industry and regulators in identifying the appropriate persons that have control over the DeFi arrangements and can be responsible for compliance. A number of respondents stated that it was not clear whether a Responsible Person could include individual developers, individual governance token holders, other token holders, or other individual participants in the development and operation of DeFi products, services, arrangements and activities.

Many respondents focused their comments on whether the entity at issue is a DAO and one respondent suggested to develop guidance on the applicability of standards to DAO.

Many respondents cautioned against identifying developers that are not responsible for the offering of DeFi services as Responsible Persons. They highlighted that developers may not have control over the DeFi arrangements or how the DeFi protocols are used by others, and holding developers responsible is not in line with existing regulatory approaches towards technology or software vendors. One respondent expressed that applying the DeFi recommendations to networks or protocols would in practice prevent the development or use of open-source or permissionless networks and protocols.

Some respondents highlighted that there may not be any Responsible Persons or anyone with control and sufficient influence over DeFi arrangements that are truly decentralised. One respondent emphasized that many of the proposed applications of IOSCO's principles are not directly applicable to true DeFi operations and expressed that in the case of AMMs and LP tokens, the tokens are not issued by natural or legal persons, but by code.

A few respondents suggested that the recommendation should clarify/specify the regulatory obligation of the Responsible Persons, such as defining the regulatory obligation based on the responsible role within the tech stack. Some respondents suggested that it would be burdensome to hold providers of DeFi products or services responsible for managing the impact of MEV, as they would not have control over or the ability to influence miners and validators of the underlying blockchain.

IOSCO Response

IOSCO agrees that regulators should evaluate all facts and circumstances, including the ability of the persons or entities to effectively control or influence the DeFi arrangement.

In regard to the definition of Responsible Persons, this set of principles is intended to provide high level guidance on possible persons that regulators may consider when assessing who is a Responsible Person to enable regulatory compliance for a regulatable activity, product or service. In applying the recommendations, a first step should be looking at what the product, service or activity is, i.e., whether it is a financial product, service, or activity. The next step is identifying if anyone in fact controls or has sufficient influence over the offer of the product, or provision of the service, or engagement in the activity. As with traditional finance, this may be an entity (whether a corporation, partnership, or other organization of persons) or an individual or both. Either of which may, for example, offer or sell a financial instrument or other investment product, or provide the services of, or engage in activities of, an exchange, broker, dealer, investment advisor, or other financial intermediary. The determination is based on whether, in fact, they control, in some way, the offer of products, provision of services, or engagement in activities, and not on how they are organized.

In analyzing who a Responsible Person is with regard to any product, service, or activity, it is important to recognize that the manner of organization of the entity or persons who control/influence a product, service, or activity, including whether their organization is a legal corporate form or is supposedly "decentralized" is not the measure of whether the actual product, service, or activity at issue is subject to regulation.

While a DAO may be decentralized in terms of its governance, the focus is on whether the DAO itself is offering a product, providing a service, or engaging in an activity. If so, the DAO, as an entity or group of persons, would be the Responsible Person with regard to the product being offered, service being provided, or activity being engaged in. The fact that a DAO may not have one person in control is no different than, for example, a general partnership or joint venture, where all participants participate in the management and operation of the partnership or venture.

After considering the feedback, the report adds clarifying language to the recommendations and guidance that, regardless of how an entity or person(s) are organized, or how decentralized an arrangement is, they may be considered to be a Responsible Person based on the characteristics described above. This approach acknowledges that each situation may

present unique circumstances and complexities that warrant individualized scrutiny and allows for a case-by-case assessment and more tailored and precise determination, ensuring that regulatory decisions are made with a keen understanding of the specific context in which they are applied.

The report has been changed to add clarifying language.

4. Disclosure

Summary of feedback

The importance of clear, accurate and comprehensive disclosure was a cross-cutting theme among all the responses. Some respondents provided specific suggestions on who should be subjected to the disclosure requirements. One respondent suggested that disclosure requirements should be imposed on entities operating applications that directly interact with users as it would incentivise these entities to assess the DeFi protocols on behalf of the users. Another respondent suggested that regulators should take an enterprise view of the ecosystem to identify appropriate Responsible Persons to provide the relevant disclosures.

In regard to the content and granularity of the disclosure, some respondents suggested that disclosure requirements should be tailored according to the complexity of the DeFi product or service as well as the sophistication of the investor while others asked for IOSCO to develop a template or gives some guidelines on appropriate disclosure for DeFi products and services.

Some respondents stated that appropriate disclosure would also help resolve the lack of standardized data. One respondent suggested expediting the implementation of Recommendation 6 (Require Clear, Accurate and Comprehensive Disclosures) to address the complexity and opacity of DeFi product, services and arrangements. This respondent asserted that disclosures would also highlight additional data that is needed for more streamlined and standardized data collection.

One respondent suggested that regulators should determine guidelines or minimum standards on disclosures for DeFi platforms. This respondent suggested that regulators should require the DeFi service providers to disclose their source code, infrastructure, and smart contracts in a way that is human-readable, or alternatively, require DeFi service providers to have their source code, infrastructure, and smart contracts audited.

Finally, a respondent suggested that IOSCO should defer to non-securities regulators on the appropriate disclosure requirements because disclosures for DeFi products and services were more similar to disclosures for consumer products rather than traditional securities.

IOSCO Response

The recommendations are designed to be principles-based and provide high-level guidance so that regulators can take into account their respective domestic landscape, mandates and applicable regulatory frameworks. IOSCO agrees that in ensuring clear, accurate and comprehensive disclosures, regulators should consider how best to tailor the disclosure requirements for their jurisdictions, including whom to impose the requirements on and the extent of disclosure requirements needed. In that regard, IOSCO agrees that regulators should give due consideration to ensuring disclosures are helpful for investors of various levels of sophistication.

Following the feedback, the recommendation has been updated to reflect that the information given to users and investors should be not only comprehensive and clear, but also concise and non-technical.

Furthermore, the guidance has been strengthened to set out that regulators should also consider how requirements account for differences in investor sophistication.

The report has been changed to add clarifying language.

5. Data, and Identification of Tokens

Summary of feedback

The majority of respondents agreed with the description of data gaps and challenges in the Report. A few respondents stated that it would be helpful to clarify the data points, types of data standardization or metrics needed to facilitate reporting, as well as how these metrics would be assessed.

A few respondents cautioned against applying regulations before fully understanding the technologies used in DeFi or otherwise disagreed with the description of data gaps. A respondent asserted that blockchain transactions are completely transparent and provide greater visibility compared to traditional financial systems, and blockchain analytics platforms could be used to analyze data.

A couple of respondents asserted that market participants can address the data gaps and challenges in the Report by using tools such as blockchain analytics platforms and relying on companies that perform economic audits and stress tests of smart contracts. One respondent suggested requiring platform developers or DeFi service providers to insert a time-lock function in the smart contract or protocol to wait for a certain amount of time before changing the source code or deploying new source code that requires them to update disclosures or changes in the DeFi platform on a continuous basis. Another respondent stated that market participants should demonstrate that they have the necessary data management arrangements in place to ensure the reliability and availability of the data used. If a market participant relies on a data provider, the provider should demonstrate a robust operational infrastructure, with well-defined processes, adequate resources and business continuity plans to ensure the reliability of the data provided.

Some respondents stated that IOSCO members can address data gaps and challenges by focusing on capacity-building to effectively monitor DeFi products, services, arrangements, and activities. A few respondents stated that regulators should use existing tools to conduct data analysis, such as blockchain-native solutions to identify specific individuals/entities and oracles to provide real-time, verifiable data. A couple of respondents suggested that regulators should receive training or participate in data sharing workshops to understand how to identify, collect and analyze the types of data needed for ongoing monitoring.

Many respondents had conflicting views on whether regulators should impose data standards or allow the industry to develop data standards. One respondent suggested that regulators should determine guidelines or minimum standards on disclosures for DeFi platforms. In contrast, a couple of respondents suggested that the industry could develop common standards for data analysis if given sufficient time to do so, or simply promote existing standards developed by the industry (e.g. ERC3643 on permissioned tokens).

A few respondents proposed a collaborative approach between regulators and industry to incentivize the adoption of data standards and improve aggregation methods by data

providers and protocols. One respondent stated that market participants should be able to choose whether to buy or build data processes without regulators mandating an approach, however, market participants should be able to demonstrate that they have appropriate systems and policies for data consumption and use, as well as effective operational risk management processes. Another respondent stated requirements could be applied to data providers through guidelines, the implementation of compliance labels, and the establishment of specific regulatory statutes, similar in purpose to those used on the financial markets. The respondent believed these measures would support the reliability and transparency of the data used in the DeFi market, facilitating more effective regulatory oversight. Yet another respondent supported the creation of a self-regulatory organization (SRO) where one does not yet exist to establish standards for facilitating data collection and distribution.

Finally, some respondents encouraged the use of digital token identifiers (DTIs) to address data gaps. A couple of them consider the ISO 24165 DTI to be an important tool for both market participants and regulators to understand unique risk profiles associated with digital tokens and blockchains. Another cited a certain standard as a way to identify counterparties in digital asset transactions and to identify holders of digital assets: ISO 17443, the Legal Entity Identifier (LEI).

IOSCO Response

Some jurisdictions have existing regulatory frameworks that encompass DeFi, while others are in the process of developing regulatory frameworks. The recommendations acknowledge these differences in regulatory frameworks, retaining some flexibility for regulatory authorities to implement the recommendations within their existing or new frameworks. This may include allocating responsibility for the regulation of DeFi to multiple regulators that have different mandates and objectives to address investor protection and market integrity risks.

Each jurisdiction should implement the recommendations by considering the regulator's role and the outcomes achieved through the operation of the regulatory frameworks in each jurisdiction. ANNEX C to the DeFi Consultation Report describes the data gaps and challenges, including examples of metrics that may be useful for analyzing DeFi protocols, blockchains, and the DeFi market more broadly. How IOSCO members will assess DeFi products, services, activities, and arrangements is the ultimate responsibility of the respective members.

The DeFi ecosystem is nascent and evolving. If the sector grows further and becomes more interconnected with traditional financial markets, it poses concerns from a financial stability perspective. There are significant data gaps and challenges that regulators and market participants face in identifying and responding to risks and developing or applying regulatory

requirements to Responsible Persons in DeFi. Existing analytical tools, data providers, and data analytics services can be used to collect, process, and analyze data.

Data transparency and regulatory reporting are integral to effective market surveillance, however, the inaccessibility of relevant data reduces the ability to monitor activity. Accordingly, the guidance under Recommendation 1 (Analyze DeFi Products, Services, Activities, and Arrangements to Assess Regulatory Responses) was expanded to acknowledge the importance of addressing data gaps and challenges to enhance investor and market protections. Regulators should consider how to apply appropriate recordkeeping and reporting requirements to Responsible Persons. Generally, regulators should apply recordkeeping and reporting obligations for financial transactions and data in DeFi that would achieve the same outcome as for traditional market participants.

The report has been changed to provide additional guidance.

6. Ongoing monitoring and collaboration between regulatory authorities and market participants given the dynamic nature of the DeFi market.

Summary of feedback

Respondents provided several suggestions regarding collaboration and interaction between regulators and market participants to avoid overly broad regulation and balancing investor protection and innovation.

Some respondents suggested that market participants should work together with regulators to develop best practices for the use and regulation of emerging technologies and products. One respondent proposed that stakeholders should collaborate to develop standards around selected risk management and governance topics such as cybersecurity risk or code audits. Another one said that in relation to cross border cooperation, the recommendations should seek further recognition of licenses issued to CASPs across borders.

Two respondents focused more on private/public sector cooperation and education. One of them suggested the development of a public-private sector working group in 2024, including technology providers and technology standard setting bodies. The other suggested strengthening the IOSCO training on crypto, through a revised Harvard certificate or the development of a new global certificate programme or a seminar training programme.

Many of the respondents highlighted the importance of cross-border collaboration and the cooperation with different stakeholders in the ecosystem. Different approaches such as a bottom-up approach or a principle-based approach were proposed to regulate DeFi, products, services, and activities.

One respondent suggested that regulators draw inspiration from their initiatives to create sandboxes, fintech offices and innovation labs. These initiatives have provided the guidance and support needed to address investor protection and market integrity risks.

Some respondents suggested the creation of cross-stakeholder working groups to rapidly implement adapted and common regulatory standards.

In regard to the ongoing monitoring of the DeFi markets, the feedback included different suggestions. Some respondents suggested the use of existing tools such as the Travel Rule which dictates that Virtual Asset Service Providers (VASP) identify the originators and beneficiaries of cryptocurrency transactions.

One respondent outlined that the existing data, such as information on the DAOs of various projects or market data, would provide a means for supervision of decentralized finance activity. The respondent further explained the usefulness of tools for identifying people and entities involved in a protocol.

Some respondents recommended using data chain analytics in evaluating DeFi ecosystem.

One respondent identified indicators such as Total Value Lock (TVL), number of users, aggregate flow, governance structure and operation, tokenomic and distribution, volume of transaction, fee or revenue and market share, and smart contract auditor in evaluating DeFi products, services, arrangements, and activities.

Finally, a respondent outlined that monitoring on-chain and collecting off-chain data would be useful in assisting authorities to monitor important trends and behaviors in the market.

IOSCO Response:

IOSCO notes the suggestions including collaboration and interaction between regulators and market participants, avoiding overly broad regulation, striking a balance between investor protection and financial innovation, and continuing to work with the industry to refine regulatory standards as the DeFi market evolves.

IOSCO takes note of the comments in favor of more international cooperation and better coordinated international framework. Moreover, IOSCO acknowledges the need for sustained collaboration with stakeholders in the DeFi ecosystem taking into account the ever-evolving nature of the market. With its broad membership of more than 130 jurisdictions, IOSCO is uniquely positioned to facilitate collaboration between regulatory authorities and react to market developments.

IOSCO also noted that common argument concerning data collection, data analytics and audits would help achieve the purposes of identifying DeFi market trends and

entities. The use of existing standards and tools has also been encouraged in evaluating DeFi activities.

No change.

7. Interoperability between the CDA and DeFi Recommendations

Summary of feedback

Several respondents highlighted the importance of interoperability between the CDA and DeFi recommendations.

One respondent expressed that while they fully support the need for IOSCO members to view the two reports as one framework, it is important to expedite and prioritize the effective oversight and supervision of CASPs that currently serve as the on and off-ramps into the crypto asset ecosystem.

Some respondents considered the interoperability between the two IOSCO reports to be a highly effective development for what they asserted were distinct regulatory frameworks tailored to specific categories of crypto assets and a separate bespoke regime for DeFi activities. They further highlighted that that such an approach might demand the creation of a different flow chart illustrating the interoperability of the CDA Report and the recent DeFi Report and to bring more clarity towards the applicability of specific principles, recommendations, and guidance.

One respondent proposed considering a nuanced decentralization spectrum rather than a binary classification between centralized and decentralized models and suggested an integrated set of recommendations covering crypto assets, stablecoins, and DeFi, with the DeFi regime being less prescriptive.

One respondent further suggested to (1) focus on establishing a global baseline of recommendations, (2) refocus on defining "decentralization" and applying the recommendations for "decentralized" protocols and centralized service providers that facilitate access to such protocols instead of conflating DeFi and centralized financial intermediaries in an attempt to defend the relevance of anachronistic approaches to regulation, and (3) omit references and language suggesting or implying the endorsement of anachronistic regulatory approaches in a final report.

One respondent expressed the view that this report serves as a logical extension of the CDA report and emphasized that both the DeFi and CDA recommendations can be read as standalone documents dealing with DeFi and with crypto and digital assets respectively.

Two respondents expressed concerns that market participants may find it challenging to navigate the DeFi Report and the IOSCO CDA Report, particularly given the possibility

that an entity may be subject to the DeFi recommendations, the recommendations in the CDA Consultation and the other IOSCO Standards to varying degrees across its activities.

Finally, one respondent expressed that applying the IOSCO Objectives and Principles of Securities Regulation to DeFi arrangements may not be perfectly suitable, as these principles may not align entirely with the reality of the DeFi market and highlighted that there could be instances where a company developing a DeFi protocol might also need to adhere to CASP requirements due to their business model.

IOSCO response:

The DeFi recommendations, considering the stage of advancement of these markets, are in general more principles-based and less prescriptive than the CDA Recommendations.

Together, the DeFi recommendations and the CDA recommendations are designed to complement each other. They provide a clear and interoperable policy framework which will help IOSCO members to achieve regulatory outcomes consistent with those required in traditional financial markets. The flow chart in the DeFi Consultation Report provides a useful means of assessing which set of recommendations should apply.

Acknowledging the importance of coherence and consistency between the CDA and DeFi recommendations, IOSCO has published an Umbrella Note alongside the DeFi Final Report, further articulating the interoperability between the two sets of IOSCO policy recommendations.

No change in recommendations. An umbrella note has been developed and published to clarify the interoperability between the two sets of recommendations.

8. Additional risk considerations related to DeFi

Summary of feedback

Respondents gave feedback on a wide range of risk and issues related to DeFi. Several participants outlined issues with know-your-customer (KYC) and anti-money laundering (AML). These included the cost of monitoring AML, the challenges posed by pseudonymity/anonymity for AML screening and KYC obligations. Some respondents pointed out significant risks of money laundering and terrorist financing due to an absence of requirements to abide by AML rules for many DeFi products and services. A respondent expressed the view that a large number of DeFi platforms operate without meaningful KYC processes or AML/CFT compliance, despite clear indications from a variety of regulators that most DeFi platforms are subject to these requirements.

A few respondents contended that there is difficulty in defining and allocating liability – and that there is a lack of responsible parties and clear accountability.

Some respondents identified smart contracts and AMMs as weak points associated with DeFi. Several respondents highlighted that smart contracts may harbour flaws that could be exploited by malicious actors (i.e., change its content) which could lead to the loss of assets stored in the affected contract (losses for asset owners).

Many respondents addressed liquidity risks and price volatility: many DeFi projects depend on liquidity provided by users. Price swings and sudden withdrawal of liquidity can cause instability and lead to significant losses.

In the same vein, two respondents stated that while the report highlights several risks associated with DeFi protocols, not all risks should apply equally to every protocol's arrangement. The combination of risks depends on the protocol's arrangements (products, market participants, governance structures, and technological setups). They further asserted that a blanket approach to assessing risk would not be an appropriate policy outcome.

One respondent argues that "nascent stage of development" should not be considered a risk in itself, although they agree that "a nascent stage of development can lead to exposure to the other risks".

Some respondents also described risks which were not directly covered in the Report. Among these there was geopolitical risk, cryptography risks, composability risk and environmental impact assessment risk.

A few respondents highlighted risks related to the management of conflicts of interest and suggested there could be more clarity on when measures such as legal disaggregation would be required. One respondent cautioned against resorting to disaggregation without due consideration to how technology in DeFi may mitigate conflicts. Another respondent

expressed the view that there may not be any conflict of interest in a DeFi protocol that is fully automated or is operating on fully decentralized infrastructure and governance.

Respondents also shared how they would mitigate some of the risks and/or issues. Some of them suggested the use of technology solutions (advanced technologies/DeFi-related technology solutions/technology compliance solutions) which could help detect potential fraud and identify various crypto-ecosystem risks, and monitor and identify unusual or suspicious activities within DeFi protocols.

A respondent proposed the idea of engineered solutions like tokenized verifiable credentials and oracles for challenges posed by pseudonymity (AML), as well as institutional adoption of DeFi protocols via permissioned, public systems. The same respondent also raised the idea that fostering the functioning of trusted digital identity solutions could mitigate KYC / anonymity challenges for DeFi arrangements and enable scalable access.

One respondent suggested that market participants should adopt real-time data technology for routine risk management and report any issues and problems immediately to the relevant authorities and IOSCO if issues occur.

Some respondents highlighted the importance of due diligence. They suggest that market participants should conduct thorough due diligence before getting involved in any DeFi project or before using such new technology or product. The importance of a careful review the smart contracts and protocols they intend to use is also underlined. To mitigate both technology and cyber risk two respondents assert that “best practices” including robust auditing procedures and code audits are critical to ensuring safe and effective operation of a DeFi Protocol.

Other respondents suggested that market participants should also work together with regulators to develop best practices for the use and regulation of emerging technologies and products or proposed that stakeholders should collaborate to develop standards around selected risk management and governance topics such as cybersecurity risk or code audits.

IOSCO Response

Respondents described and commented on a wide range of risks and issues around DeFi protocols. They provided numerous technical details and additional information on risks, proposed different types of solutions and gave numerous examples. They also highlighted what they considered to be best practices and standards, as well as measures adopted by the industry to mitigate risks.

Nonetheless, IOSCO has noted a certain degree of consensus with the risks and issues associated with DeFi protocols identified and on the importance of acting in the face of the risks and issues associated with associated with DeFi protocols.

Overall, opinions differ as to the types of measures (i.e., prescriptive requirements, best practices, guideline or industry standards/ guidance) that should be taken to address the risks and issues as well as for the need for regulators to take action at this stage.

The DeFi Final Report provides a diagnostic and prognostic 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. The regulatory approach to DeFi continues to adapt in response to emerging risks arising from technological advancement. IOSCO remains interested in understanding how new technological solutions can help mitigate some of the risk identified.

In regard to the points related to conflict of interests, IOSCO disagrees that the automation of a DeFi arrangement or the presence of a decentralized governance model would necessarily eliminate conflicts of interest. Individual persons or entities may take on different roles and capacities within a DeFi arrangement which may still give rise to conflicts of interest. Additional text has been added to the guidance of Recommendation 4 to emphasize the present risks of conflicts where various activities are performed by individual persons or entities within a DeFi arrangement, notwithstanding a greater degree of automation and decentralized governance.

Finally, IOSCO acknowledges that legal disaggregation need not be used as a blanket measure to address conflicts of interest and recognizes that vertical integration of DeFi services could still exist so long as regulators assess that effective mitigation of conflicts can be done through other measures.

The report has been changed to provide additional guidance.