euci European Crypto Initiative Canadian Web3 Council BHARAT WEB3 ASSOCIATION BLOCKCHAIN ASSOCIATION SINGAPORE

October 19, 2023

Mr. Jean-Paul Servais
Chair of the IOSCO Board
International Organization of Securities Commissions (“IOSCO”)
C/ Oquendo 12
28006 Madrid, Spain

VIA EMAIL: deficonsultation@iosco.org

RE: Public Comment on IOSCO’s Consultation Report on Policy Recommendations for Decentralized Finance (DeFi) (“the Consultation Report”)

Dear Mr. Servais

The European Crypto Initiative (EUCI), the Canadian Web3 Council (CW3), Blockchain Association Singapore (BAS), and Bharat Web3 Association are pleased to respond to the IOSCO’s Consultation Report.

EUCI is an advocacy organization based in Brussels, Belgium, that aims to shape EU regulation to favor open, permissionless, decentralized applications leveraging blockchain technology while advocating for an innovative EU environment, supporting technological development for SMEs and innovative crypto-assets service providers (CASPs).

The CW3 is a non-profit trade association founded by industry leaders to work constructively with policymakers and establish Canada as a leader in Web3 technology[1]. The CW3 represents organizations that have made a critical impact on the development of Web3 technologies across the globe and who are committed to responsibly building and innovating in Canada. Our membership is diverse, ranging from hackathon organizers to financial products, trading platforms and investors, and open-source blockchain projects.

[1] At its core, web3 technology aims to enable direct interactions between users without relying on intermediaries. It emphasizes the use of decentralized applications (dApps) that run on blockchain networks, where data and processes are distributed across a network of nodes, making them resistant to censorship, manipulation, and single points of failure. Overall, web3 technology represents a paradigm shift towards a more decentralized, open, and user-centric internet, empowering individuals and communities with greater control over their digital lives.

The BAS seeks to empower its members and the community to leverage blockchain and scalable technologies for business growth and transformation. The Association is designed to be an effective and inclusive platform for members to engage with multiple stakeholders – both regional and international – to discover blockchain-based solutions and promote best practices in a collaborative, open, and transparent manner. It aims to promote blockchain literacy for the digital economy in Singapore.

Bharat Web3 Association is the apex body for the leading Web3 technology companies in India, with the aim of leveraging blockchain and scalable technologies to accelerate growth and transformation in India. It advocates for collaboration between the regulatory bodies and the Industry to create awareness about the new age technology and the emerging asset class. The mission of Bharat Web3 Association is to help India realize its vision of being the leading digital economy.

Consultation with affected stakeholders is essential to effective policy-making and ensuring the regulatory framework and the regulations are fit for purpose. We appreciate the opportunity to provide you with our comments and insights. We hope global regulators and standard setters will find the comments useful in shaping a modern regulatory framework(s) and regulations for decentralized finance.

Executive Summary

We appreciate the efforts by IOSCO, using its influence as a global standard setter to lead this initiative from a DeFi perspective. We encourage greater coordination amongst regulatory bodies (both globally and nationally) given the intersections between DeFi protocols with both traditional financial markets and centralized finance.

We support a principles-based and risk-based approach to regulation that emphasizes full disclosure of risks, impacts, and benefits to users. Recognizing the dynamic and evolving nature of DeFi and DAOs, we support a regulatory approach that prioritizes proactive guidance and collaboration over punitive measures. A policy approach that balances the competing interests of stakeholders acknowledges the risk mitigation measures, and monitors for any residual risks can help foster innovation and responsible growth in the rapidly evolving landscape of decentralized finance.

1. We recommend adopting a **“same activities, same risks, same regulatory outcome”** rather than a “same activities, same risks, same rules” methodology. We believe that a bespoke regulation would be far better at encapsulating the nuances of DeFi rather than just reproducing the rules applicable to traditional finance and financial intermediaries. See response to Q1.

2. We believe that there are common misconceptions as a consequence of perceiving DeFi to be the antipode of CeFi. While any classification benefits from the identification of two contrasting concepts, the evolution of DeFi strongly suggests we consider **decentralization as a spectrum**. Acknowledging the varying degrees of decentralization, particularly over a project’s life cycle, allows for the recognition of a wide range of components (e.g. operational and managerial autonomy) and trade-offs with unique sets of features and risks. Identification of such components and factors can contribute to a more profound and flexible regulatory framework that applies under specific conditions. See response to Q2.

3. With decentralization existing on a spectrum, the governance models should also be considered on a spectrum. We encourage regulators to consider the possibility that with DeFi protocols, there may not be a “natural person or entity” to regulate. We caution against imposing regulatory obligations relating to governance protocols, particularly in the settlement layer, which supports many applications. A strong method of classification and evaluation of various governance mechanisms should be developed to ensure that the network operates in a secure and stable manner. See response to Q3.

4. We believe that risks can be deconstructed into an equation comprising threat severity, probability of occurrence, and impact. Risk should be evaluated through the lens of effective mitigation measures. We note some additional risks in our response to Q4.

5. We acknowledge that there are currently some data gaps. However, the use of advanced analytics tools can make data interpretation more straightforward and meaningful. In addition, implementing a decentralized ID system could provide a balance between user privacy and regulatory needs. See response to Q9.

6. With respect to the application of IOSCO Standards to DeFi activities, we note that many principles listed are clearly relevant to DeFi activities, given the parallels between traditional finance markets and decentralized markets. We support the adoption of IOSCO principles where appropriate. However, there are examples and principles that cannot easily be reproduced in the context of DeFi, or that may not be appropriate for the type of activity (e.g. asset-based borrowing/lending DeFi assets) or the type of crypto asset used as collateral. A new regulatory framework (or principles) may be needed in such cases. See response to Q6.

7. We note that there are technological innovations that allow regulators to support innovation in DeFi/blockchain technologies while at the same time addressing investor protection and market integrity risks. Specifically, there are ways in which various audit or assurance activities could support innovation within this space. In addition, there are blockchain explorer and analytics platform tools such as Etherscan and those created by the Cardano Foundation that can be used to gain insight into DeFi/blockchain technologies. See response to Q8.

8. We note that there are several methods or mechanisms that regulators can use in evaluating DeFi products, services, arrangements, activities, and other persons and entities involved with DeFi. See response to Q9.

9. We would recommend (i) guidance on documentation of processes, management, and bundles of smart contracts, (ii) standards for smart contract verification, and (iii) guidelines around the exchange of data gathered from auditors when assessing security levels and compliance on the technical side. See response to Q7.

We applaud IOSCO for ensuring that there is interoperability between the DeFi report and welcome further exploration of various trade-offs or combinations between decentralized activities and services offered by CASPs.

Q1: Do you agree with the Recommendations and guidance in this Report? Are there others that should be included?

A scenario where strict top-down regulation leads to industry-wide negative reactions and eventual repeal of the proposal, as was the case with CFTC's Automated Trading Regulation, should be avoided in the case of DeFi. After the 2008 financial crisis, the CFTC attempted to impose a strict and comprehensive risk management regime on trading algorithms under immense political pressure. However, the proposed regulation was deemed too complex, overreaching, inconsistent, and disincentivizing to innovation. The proposal was amended in 2016 and completely withdrawn in 2020.[2] This example shows that when it comes to the regulation of new, disruptive technologies, a politically motivated top-down regulation can stifle the adoption of new technologies and the full exploitation of their market potential. Therefore, in our opinion and following this example, a politically neutral, bottom-up approach should be the only way to regulate DeFi effectively. To assist IOSCO members in complying with IOSCO Recommendations, we provide detailed insights and additional guidance for each specific recommendation in our response to Question 7 below.

[2] Hess, Eric, Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation (September 13, 2023). 128 PENN ST. L. REV. 2 (forthcoming Feb. 2024), page 20. Available at SSRN: https://ssrn.com/abstract=4571106

Q2: 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.

In response to the question regarding the description of DeFi products, services, arrangements, and activities outlined in this Report, we have divided our response into three distinct sections to offer a comprehensive assessment. These sections will delve into the following aspects: 1) decentralization as a Spectrum, 2) Collection of Fees, and 3) Crypto-Assets Used in Lending/Borrowing Activities.

1. **Decentralization as a spectrum**

We commend IOSCO for its comprehensive summary of common products and services using DLT, both in the 2022 and the most recent 2023 Report. While the report strongly emphasizes technical and transactional aspects, it's worth noting that the typology of transacted crypto-assets is not covered within the current scope, which underscores the need for a local classification of crypto-assets and a consolidated worldwide report on that matter.

We further posit that numerous misconceptions, as detailed in Section II of the Report, stem from the historical perception of DeFi as a diametrically opposed counterpart to CeFi. However, the dynamic evolution of DeFi underscores two key insights:

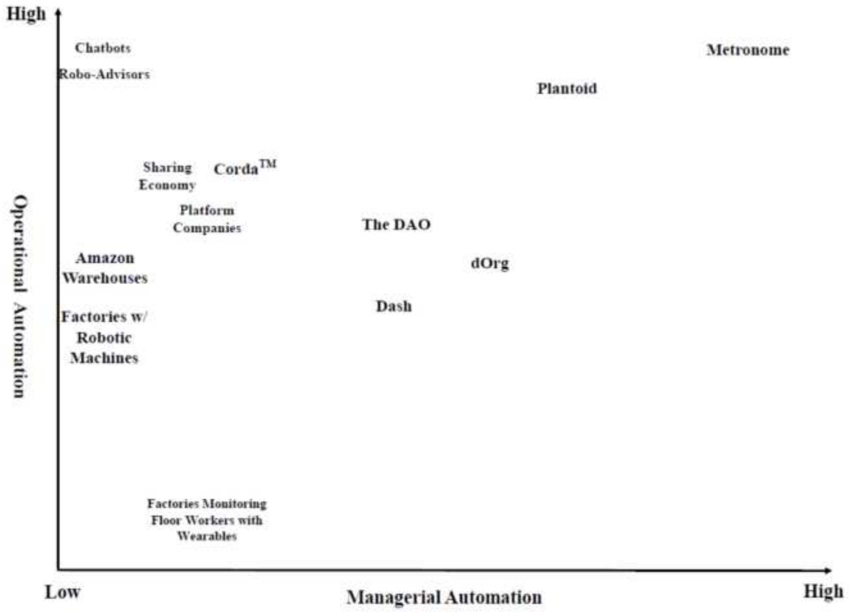
- Decentralization Spectrum: The concept of decentralization is better understood as a spectrum, not a binary choice.
- Synergy Between DeFi and CeFi: It's crucial to recognize that DeFi and CeFi are not inherently in conflict; in fact, they can complement each other harmoniously.

To fully unpack and understand the decentralized nature of various entities, one should think of it as a scale, whereas fully decentralized and centralized present extreme ends of the same line. We do believe that a decentralized foundation is a prerequisite for DeFi.[3] A thorough understanding of the (absence) of control structures in DeFi is key for the regulators and institutions considering their participation or regulation of the ecosystem. Understanding that the

[3] Schuler, Katrin and Cloots, Ann Sofie and Schär, Fabian, On Defi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance (April 18, 2023). Available at SSRN: https://ssrn.com/abstract=4422473 or http://dx.doi.org/10.2139/ssrn.4422473

technical design of DeFi and the technological stack does not present a mere technicality, there may be various centralization vectors that are inherited through the dependencies on the lower layers of the technology stack. Additional centralization parameters are described in the article titled Autonomous Business Reality,[4] where Prof. Carla L. Reyes elaborately describes both operational and managerial automation design tradeoffs undertaken by the protocol or nodes, as well as business owners, founders, managers, users, and other individuals. Prof. Reyes observes that the companies are "*willing to experiment with emerging technologies are quietly testing systems built on blockchain technology and artificial intelligence that promise to radically improve the proxy system.*" Even though not based on a strictly mathematical formula, Figure 1 below shows the Autonomous Business Map, which reveals clusters of autonomous businesses and places various protocols on a scale of managerial and operational automation. It also reminds us that protocols' aims are not monolithic and that the means to achieve their purposes vary significantly in practice.

FIGURE 1:[244] AUTONOMOUS BUSINESS MAP



Source: Reyes, Carla, Autonomous Business Reality (2021). 21 Nevada Law Journal 437 (2021), SMU Dedman School of Law Legal Studies Research Paper No. 479, Available at SSRN: https://ssrn.com/abstract=3574988

[4] Reyes, Carla, Autonomous Business Reality (2021). 21 Nevada Law Journal 437 (2021), SMU Dedman School of Law Legal Studies Research Paper No. 479, Available at SSRN: https://ssrn.com/abstract=3574988

On this note, we again welcome the assessment criteria proposed by the authors of the Report, and we wish to point out that the regulators should not strive to make a strict distinction between two contrasting examples, the so-called “fully decentralized” protocols and those that provide central points of operation. Instead, decentralization is a spectrum that changes over time and depends on technological layers and the level of control or the nature of interference one can exhibit. The spectrum itself results from various design or function tradeoffs between consensus protocols and a code's (in)completeness. Tradeoffs can also be made between multiple business organizations or when hiring more staff is prioritized over product design.

Furthermore, as pointed out by OECD in their 2022 article “Why decentralized Finance (DeFi) Matters and the Policy Implications”[56] DeFi protocols often start as centralized projects and gradually decentralize as the community of users/developers grows, and the development of the protocol increases in both scope and size. The movement through the decentralization spectrum is the inherent and natural development cycle of most DeFi projects. On this note, it is necessary to emphasize that the level of decentralization within the settlement layer sets the maximum limit for all projects constructed on top of it (the so-called inherited centralization vectors).[7] For enhanced clarity and ease of visualization, we have included a graphic illustrating the technology stack adopted by Prof. Dr Fabian Schär:[8]

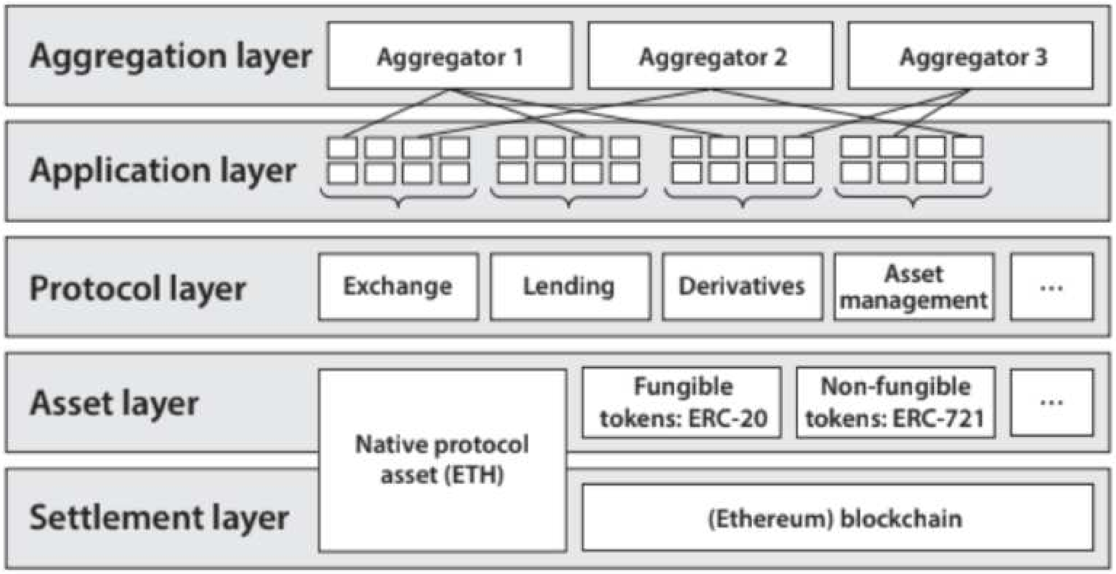
[5] OECD, `Why decentralized Finance (DeFi) Matters and the Policy Implications', page 21.

[6] IOSCO, “Decentralized Finance Report”, March 2022, page 10.

[7] Schuler, Katrin and Cloots, Ann Sofie and Schär, Fabian, On Defi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance (April 18, 2023). Available at SSRN: https://ssrn.com/abstract=4422473 or http://dx.doi.org/10.2139/ssrn.4422473.

[8] Schär, Fabian, Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets (March 8, 2020). Available at SSRN: https://ssrn.com/abstract=3571335 or http://dx.doi.org/10.2139/ssrn.3571335.

The DeFi Stack



Source: Schär, Fabian, Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets (March 8, 2020).

Further, when projects build on top of a decentralized stack of technologies, they may use avenues to access specific applications or aggregator services. Such avenues may already fall under existing rules and regulations and present the access points that can be subject to New Frameworks. We deem it crucial to limit the regulatory intervention to those technological stacks that exhibit a high level of centralization only.

However, instead of making a delimitation between two extremes (i.e. fully decentralized vs. not fully decentralized), we believe the regulatory framework should consider a different typology that considers decentralization as a spectrum that depends on centralization vectors as solid indicators of potential regulatory intervention. To do so, the regulator should identify various examples and define a typology through which tradeoffs are linked to other risks, demanding specific compliance regimes. Hence, instead of evaluating whether an activity falls within the remit of (fully decentralized) DeFi, we ask the regulators to assess a spectrum of decentralization and thus apply the compliance requirements accordingly.

We further believe that to support innovation in the field of DeFi properly, and regulators should keep in mind the process of inherently changing the decentralization level of protocols and adopt the regulation in a way that would not (intentionally or accidentally) set any unnecessary legal barriers for this process. Responsible persons, e.g., developers and project initiators, should not have to constantly monitor the degree of decentralization, appropriate legal documentation, or ask for specific permissions every time a certain decentralization threshold is crossed. On-chain centralized activities, products, and services come with novel control structures, while genuine decentralized activities have no centralized controlling entity and, therefore, no regulatory hook.

2. Collection of fees

When expounding on DEX providers and AMM operators, the Report further states that the "*operator typically collects fees for makers and takers for providing this service*." We wish to note that several of the most notable DeFi products or services are offered in a way where the fee is not charged by the operator but collected through a protocol or an interface. Most notable examples include Uniswap, the largest decentralized exchange protocol that has so far amassed more than 1.6 trillion USD in transactions, and a market leader AAVE that has earned more than 603 million USD in protocol fees since its inception.[9] These are not the operator's fees. It is crucial to understand that no centrally managed operator charges a fee in such cases and gains economic benefits. As such, these fees should be strictly differentiated from any other financial instruments. These protocols, their tokens, and fees exhibit strong decentralized characteristics and should not fall under the scope of Existing regulatory frameworks. Any New Framework that navigates such protocols should rely on the substance over form principle and should be constructed as an *ad hoc* bespoke regime that incentivizes competition and promotes further innovation and decentralization within this ecosystem.

3. Crypto-assets used in lending/borrowing activities

When assessing the lending/borrowing services, it is particularly noteworthy that this Report contemplates a specific type of borrowing/lending activity, i.e. asset-backed lending rather than traditional bank lending where credit decisions are made based on the strength of the borrower's balance sheet and credit rating. In this context, we believe the description should

[9] Hess, Eric, Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation (September 13, 2023). 128 PENN ST. L. REV. 2 (forthcoming Feb. 2024), page 34. Available at SSRN: https://ssrn.com/abstract=4571106

distinguish between the type, quality, and amount of the crypto asset borrowed or used for collateral. Accordingly, the regulatory principles to be established should also be appropriate to this type of lending activity.

Simply applying a securities regulatory framework to this activity may not be suitable, as we note that the current IOSCO principles do not sufficiently address this type of activity from a borrower/lender perspective. For example, in some jurisdictions currently, there are prohibitions on the on-lending of crypto assets and the use of leverage on crypto asset trading platforms. We encourage regulators to resist path dependency when setting the regulatory framework for asset-based lending/borrowing protocols. However, the DeFi lending/borrowing ecosystem can intersect with crypto trading/financial markets (depending on the type of collateral accepted). So, the regulatory/supervisory framework will need to address these intersections.

We believe that the principles should also focus on consumer protection, with complete and adequate disclosure of the following: borrowing, liquidation, and repayment terms, including how collateral is held and managed, risks and benefits, pricing oracles (including pricing sources, how gathered, valuation time and frequency) and any exception handling processes. An understanding of the flow of funds is also critical. We encourage greater collaboration amongst regulators to establish principles appropriate for asset-backed lending/borrowing and to allocate supervisory oversight accordingly.

Q3: Do you agree with the Report's assessment of governance mechanisms and how they operate in DeFi? If not, please provide details.

Although we welcome the extensive work done by IOSCO in analyzing the matter, we do not fully agree with the Report's assessment of governance mechanisms and their operation in the DeFi space. Here are our specific concerns:

1. **Comparative Analysis and Concern Listing:**

The Report relies heavily on traditional governance structures for its comparative analysis. This approach might need to be reevaluated to capture the nuances and uniqueness of DeFi governance structures.

2. **Governance Mechanisms Spectrum:**

Furthermore, the Report presents governance mechanisms as predominantly stringent. It's crucial to understand that decentralization exists on a spectrum, and so do the governance mechanisms underpinning it.

3. **Need for a Robust Classification and Evaluation Method:**

Given the diverse nature of governance mechanisms in DeFi, a better strategy might prove one focused on the development of robust methods of classification and evaluation. Such methods, mainly if developed by acknowledging the feedback from the broader crypto community, would ensure that networks operate securely and stably without the risk of suppressing innovation by overregulation.

4. **Layer 1 (Settlement Layer) Governance – Annex D Observations:**

Furthermore, we would like to stress the importance of the work done by IOSCO in analyzing DeFi governance mechanisms from both technical and regulatory perspectives. However, some essential considerations might have been overlooked:

Potential for Inherent Centralization: Regulating DeFi governance at any of the technology stack layers (including the settlement layer) could inadvertently promote centralization, undermining the very ethos of DeFi. It's essential to recognize that many blockchain protocols initiate with a centralized approach and naturally evolve towards decentralization. Imposing legal mandates that encourage centralization at this foundational layer could be detrimental to the organic development of a DeFi project. It would bring forward further risks related to centralized governance.

Broad Use of Settlement Layer: We would like to point out that the settlement layer isn't exclusive to DeFi. Instead, it facilitates a myriad of applications. Imposing DeFi-specific restrictions on this layer would likely lead to overregulation, as it would be akin to regulating all entities in a building just because one tenant – a bank, in this case – resides there.[10]

Q4: 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?

We commend the authors of the IOSCO report for their comprehensive and insightful analysis of the risks associated with DeFi and DAOs as per Annex E. These risks manifest at various levels. They pose potential threats to multiple stakeholders and are inherently a result of the early development stage of the technology.

When assessing the risks and evaluating what regulatory actions should be taken to mitigate those, we note that there are four elements the regulator should take into account: (1) threat severity, (2) probability of occurrence and damage, (3) impact such risks may have, and (4) mitigation measures (already) available to the market participants. It is imperative that regulators thoroughly grasp all elements of the risks before contemplating any new regulatory interventions.

We further believe that the majority of the existing risks can be adequately managed through non-coercive measures, such as the issuance of regulatory guidelines and engaging in consultative processes through institutions such as regulatory sandboxes and safe harbors.

[10] For more details, see Schuler et al.: On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized. Finance, page 18.

Further, the IOSCO report describes the liquidity staking concentration of validators' risk with an emphasis on the Lido protocol. We observe that, indeed, approximately 31% of staked ETH is staked through Lido's software. However, individuals can choose the software they wish to use to stake their ETH. Additionally, while Ethereum is Lido's primary focus, the platform currently supports several other Proof of Stake networks, including Polygon, Solana, Polkadot, and Kusama.

It is imperative to note that:

1. Lido's protocol is non-custodial and does not hold or control any ETH that belongs to stakes.
2. Lido protocol is a self-service middleware that extends the functionality of the Ethereum mechanism to write data on the blockchain through validation and enhances the accuracy and integrity of the data written into the blocks. As such, it has no means of controlling the behavior of validators or the node operators that run them or affecting outcomes on the Ethereum network other than extending the validation capability of the network through improved access to participate in consensus and increasing the number of validators.
3. Lido's protocol enables activating new validation keys by staking in amounts less than the minimum 32 ETH. This contributes to a larger number of validators actively validating transactions, enhancing the temper resistance of the network.
4. Lido DAO conducts a public KYB role and picks the node operators through a whitelisting process before admitting them to use the software. In doing so, Lido's delegated committee of contributors checks node operators against several publicly available criteria, including the potential to be a "bad actor" and minimum technical competence, thus providing a valuable public service.

Once again, we note how crucial it is that the regulators consider the numbers and reports through the lenses of all various circumstances leading to the situation. Further, we deem it absolutely necessary to observe the measures adopted by the industry to mitigate the risks and take that into account when considering the potential applicability of Existing Frameworks or New Frameworks. We believe that at this point, any such application of regulatory frameworks would be premature and may severely handicap those that are working towards improvements of protocols and minimization of risks, including liquidity staking concentration of validators risks as described in IOSCO's latest Report.

The principle of 'same activities, risks and regulatory outcomes' may not be applicable where the circumstances causing similar activities and risks are different and the mitigating measures have already been adopted. We wish to emphasize that the promulgation of guidelines may have a far greater positive impact and can additionally incentivize the development of technical solutions that enhance the safety and responsible evolution of DeFi (and DAOs).

Further, we wish to shed some light on Annex A of the IOSCO Report, which revolves around recent events that have left a mark on the DeFi landscape, including specific mentions of Terra (LUNA), FTX, and the USDC de-pegging incident. While it is indeed valuable to highlight these events, we find it necessary to provide a critical perspective on their descriptions and implications within the context of the report.

- **Terra (LUNA) and Stablecoins:**

The report tends to portray Terra (LUNA) and its recent price fluctuations as a potential risk to the stability of DeFi. While it is true that stablecoins play a crucial role in the DeFi ecosystem, the assessment of Terra's stability mechanism may have been somewhat overstated. Stablecoin pegs can indeed face challenges, but the report should isolate Terra's mechanism from other stablecoins. The regulators should refrain from extrapolating a general rule from this specific example.

- **FTX and Scams in the DeFi Space:**

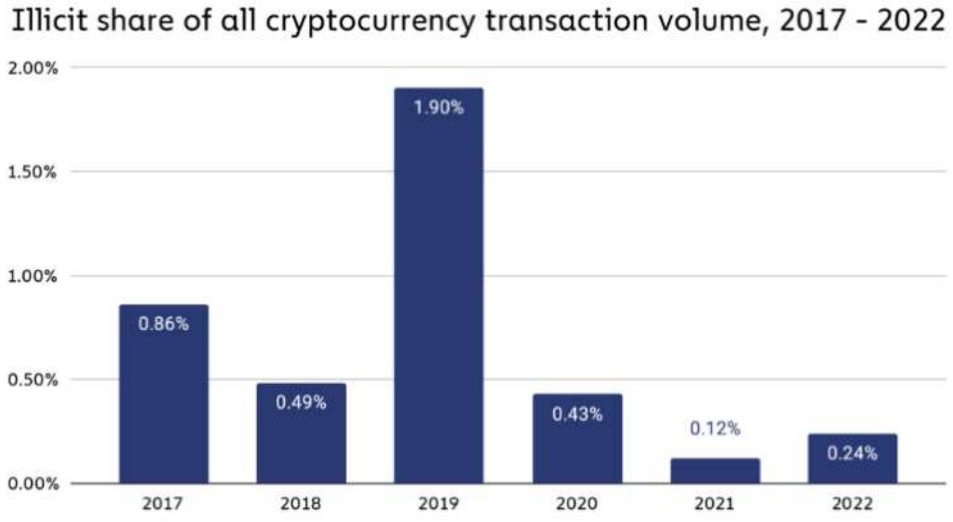
The FTX incident should be marked as a fraudulent activity highlighting the risks associated with centrally managed corporations. Classifying FTX as a rogue entity rather than a representative example of DeFi would be far more accurate. The DeFi industry takes great strides to maintain trust and security, and labelling FTX as a DeFi example could potentially mislead readers into conflating legitimate DeFi projects with fraudulent ones.

- **USDC Deppegging and DeFi's Relationship with Traditional Finance:**

While the USDC de-pegging incident is mentioned in the report to demonstrate how DeFi can be impacted by traditional financial pressures, the report might benefit from a more nuanced perspective. This incident highlights the vulnerabilities within traditional finance, indicating that reliance on traditional banking systems poses a risk to DeFi mechanisms. A more balanced portrayal would recognize that DeFi offers unique solutions and resilience precisely because it aims to reduce reliance on centralized financial systems.

- **DeFi Exploits, Attacks, and Illicit Uses**

While blockchain analytics firms report that the attacks on DeFi protocols accounted for 82,1% of all crypto-assets stolen by hackers in 2022, such isolated numbers fail to provide a clear picture of how blockchain technology and cryptocurrencies are used today. According to the latest 2023 Crypto Crime Report, the illicit activities in cryptocurrencies present a small share of overall volume - less than 1% of all cryptocurrency transaction volume is illegal. It’s also worth remembering that, despite this year’s jump, crime as a share of all crypto activities is trending downwards. The 2023 Crypto Crime Report provided by Chainalysis digs into the criminal activity behind that 0.24%.



© Chainalysis

Source: 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking, January 12, 2023, by Chainalysis, available at: https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

In conclusion, while Annex A provides valuable insights into recent events within the crypto ecosystem, a more nuanced and balanced perspective is needed to avoid potential misinterpretations and to portray the resilience and strengths of the DeFi ecosystem accurately. Incidents described in the Report exemplify the advantages brought by DeFi, which relies on a network of smart contracts and distributed ledger technologies. This reliance allows the transacting data to be immutable and publicly available to everyone. Such transparency and on-chain management of funds are crucial and seem to exhibit a greater discipline than the legal agreements, especially when backing loans and automatically executing payments to creditors. By employing proper fund separation and transparent management practices, DeFi has the potential not only to prevent insolvencies but also to shield companies from financial distress long before creditors become aware of such issues. With this in mind, we advocate for a balanced approach that prioritizes proactive guidance and collaboration over punitive measures, recognizing the dynamic and evolving nature of DeFi and DAOs. Such an approach will foster innovation and responsible growth while balancing the interests of all stakeholders in the rapidly evolving landscape of decentralized finance.

Q5: 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?

Please refer to our response provided under Question 9.

Q6: 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?

We agree with the authors of this IOSCO Report where they state that the application and/or implementation of these IOSCO recommendations can happen through the setting out of "*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.*" We believe principle-based expectations, soft regulatory guidance, or a bespoke regulatory regime are far more acceptable than a cogent regulatory framework, which may be far too premature.

This is particularly so in cases where the settlement layer or other stacks, including applications and aggregators, are provided in a decentralized manner with no centrally operated manager exhibiting control. When assessing how the existing or new frameworks are to be "applied where appropriate", it should be noted that many of the DeFi activities do not fall squarely under the existing frameworks and may be subject to a "progressive decentralization" or, in fact ", progressive centralization". For example, lending and borrowing may not fit a securities framework or financial instruments. However, the DeFi lending/borrowing ecosystem may intersect with trading or financial markets. Instead of applying IOSCO Standards and building regulatory solutions bottom-up, we deem determining the most effective allocation of regulatory responsibility more prudent.

With this in mind, we wish to remind the authors of the main design aspects, which allow us to assess the degree of (de)centralization and the existence of regulatory hooks. When determining regulatory responsibility and the possibility of effectively enforcing regulatory frameworks, the regulator should evaluate potential communication or access restrictions to the layers of the technology stack, whether anyone can verify the authenticity and integrity of transactions, and how the network agrees on the shared state of the network. Any type of restrictions, such as blacklisting/whitelisting, expropriation, emergency terminations, or interruptions of smart contracts and upgrade functionalities present centralization vectors.[11] If and when DeFi mechanisms exhibit a lack of such functionalities, the "same activities, same risks, same regulatory outcomes" cannot apply by design.

Q7: Is there any additional guidance that you would find relevant to help IOSCO members comply with these Recommendations? If so, please provide details.

To assist IOSCO members in complying with IOSCO Recommendations, we provide detailed insights and additional guidance for each specific recommendation:

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

- Taking into regard Recommendation 1 and the notion of decentralization being a 'spectrum' rather than a static characteristic of an arrangement, we welcome additional guidance on analyzing the process and stages of decentralization and acknowledgment of systemic, technical, and social risk mitigation activities. While the industry has already adopted a common practice of publishing extensive documentation regarding its products and services, it would benefit from additional support, guidelines, and standards on how such documentation should be properly maintained, publicized, and provided to the end users.
- To prevent jurisdictional arbitrage resulting from the uncoordinated, fragmented, and cumbersome approaches taken by various regulators, we recommend that IOSCO issues clear guidelines delineating instances where the Existing Framework or where a New Framework may not be necessary or appropriate. Additionally, if and when Existing Frameworks are to be applied, it is imperative to address the potential retroactive application of rules and provide guidance on how this should be mitigated properly and prevent individuals from being held responsible for legal uncertainty.

[11] Schuler, Katrin and Cloots, Ann Sofie and Schär, Fabian, On Defi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance (April 18, 2023). Available at SSRN: https://ssrn.com/abstract=4422473 or http://dx.doi.org/10.2139/ssrn.4422473

Recommendation 2 – Identify Responsible Persons

- We believe that the definition of Responsible Persons, which "*include those that maintain control or sufficient influence over a particular DeFi arrangement or activity*", could suffer from vagueness. Specifically, the precise threshold for what constitutes "sufficient influence" should be clarified. Noting that different types of controls (and influence) come with different duties and responsibilities, we deem it crucial to expand on what constitutes the 'exercise of control' and 'sufficient influence.' The regulators should examine factors through the lenses of the so-called progressive decentralization, as already observed in the IOSCO Decentralized Finance Report issued on March 2022 on page 10, considering how the role of a 'responsible person' changes over time and what type of control imposes which type of risk. The regulator should consider residual risks, acknowledging that this technology relies on some of the most intricate incentive mechanisms and mathematical equations, which may only reveal potential vulnerabilities over an extended timeframe. It is crucial not to impose penalties on innovators pushing technology's boundaries. Instead, a fair and balanced approach is needed.
- We also deem it important for the IOSCO and other regulators to note that the governance mechanisms currently used for DeFi arrangements may as well be self-implementing. Several blockchain projects and platforms have notable self-implementing mechanisms or decentralized governance features. When software operates autonomously and a smart contract operates independently without management, control, or support from a discernible entity, the concept of a Responsible Person becomes obsolete. Blockchain technology has facilitated the development of software systems devoid of central governing authorities. These solutions and tools are frequently provided open-source, ensuring accessibility to a global audience without temporal or arbitral constraints.

Recommendation 3 – Achieve Common Standards of Regulatory Outcomes

- We deem Existing Frameworks for financial instruments, including securities, market intermediary activities, collective investment schemes, exchanges and trading systems, and clearing and settlement entities, insufficient and inapplicable to DEXes and AMMs. While the Report expands on the type of Existing Framework that is potentially applicable, we highly recommend the regulator provide clear and real case examples of how Existing Framework should apply to responsible persons and how they are expected to comply with the legal requirements.

Recommendation 4 – Require Identification and Addressing of Conflicts of Interest

- Further guidelines are needed to recognise the appropriate Responsible Person responsible for identifying, managing, and mitigating conflicts of interest (see our comment above re Recommendation 2).

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

- Similar to our comment above regarding Recommendation 4, we believe further guidelines are needed to identify which Responsible Person can identify which risks.

Recommendation 6 – Require Clear, Accurate, and Comprehensive Disclosures

- We fully understand the need for transparency when it comes to technological risks and the need for disclosure; however, we wish to bring the attention of the regulators to the issue such disclosures may cause when communicated publicly. Premature public disclosure of technical vulnerabilities may sometimes lead to more significant risks of projects and their protocols being exploited. To prevent such negative externalities, Recommendation 6 could be additionally equipped with examples of best practices and guidelines on how to provide and manage disclosures properly.

Recommendation 7 – Enforce Applicable Laws & Recommendation 8 – Promote Cross-Border Cooperation and Information Sharing

- With regards to the regulators considering "whether their regulatory framework captures whatever activity is occurring in their jurisdiction", we wish to kindly encourage the regulators to be less restrictive and adopt common standards when it comes to such situations.
- While cross-border cooperation is promoted, the Report and recommendations should seek further recognition of licenses issued to CASPs across borders.

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

- We consider Recommendation 9 significant. We believe that assessing interconnectedness is pivotal, as it can help avoid duplicative efforts by responsible parties. When responsible individuals have already disclosed risks and initiated appropriate mitigation measures, it may be unnecessary for their third-party service providers to duplicate these efforts. Regulators would have already received comprehensive information to address and mitigate risks effectively.
- With this in mind, we encourage regulators to examine situations where interconnectedness can reduce compliance and regulatory burdens imposed on SMEs and other entities or individuals offering DeFi products, services, arrangements, and activities.

Q8: 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.

An important technological innovation is vested with security assessments, commonly known as ‘smart contract audits.’ Today, smart contract audits serve as a valuable means to assess the security and functionality of smart contracts. The audits involve thoroughly revising the smart contract code and identifying any vulnerabilities or weaknesses in the code that attackers could exploit. Smart contract audit firms specialize in reviewing and analyzing smart contracts' security, functionality, and efficiency. They check whether the code does what it’s supposed to do and doesn’t result in things it is not supposed to do. Auditing firms do not, however, evaluate whether the source code is compliant with the law or whether the business model is viable. Their main objective is to prevent hacks or understand and reverse-engineer the hack when it occurs. Security revision is standard practice before the smart contract is deployed and ready for production. It is important to note that these types of security checks often demand an individual or an auditing firm to combine the latest knowledge of existing cutting-edge technology and potential solutions, as well as existing and potential exploits thereof. The auditors combine tools and innovative technological solutions to keep up to date and conduct the analysis as thoroughly as possible. At the cutting edge of cryptography, there is an inherent challenge in knowing with absolute certainty whether every aspect of audited work is effective. Auditors encounter uncertainties, such as potential issues with zero-knowledge proofs, where their reliability and mathematical validity are not yet fully established. Some vulnerabilities may have been part of the smart contracts' code for years. Yet, no one exploited them before, and no one recognized such specifications as potential or actual vulnerabilities. A good example of that might be the latest Read-Only Reentrancy feature, which has been exploited only recently, even though it has existed since its early beginnings. As the code is immutable, there's another important limitation of an audit or formal proof mechanic. The vulnerabilities cannot always be fully removed, but our comprehensive understanding can contribute to a much lower impact on the operations and execution of the code.

Rigorous research, collaboration with the experts, and continuous strengthening of the understanding and techniques additionally contribute to different specializations and expertise among the auditors. While auditing processes and evaluation criteria can vary among auditing firms, there have been instances that showcase the potential for broader reputation building. One such example is the Rekt Database. However, the information available in this public database may not be updated in real time.

The work of auditing firms and collaboration between professional auditors and regulators is crucial to understanding the overall life cycle of the technology at hand. The continuous emergence of new threats and the discovery of new bugs/malfunctions suggests there's a need for an appropriate certification process, which may demand an audit be done frequently or when certain conditions are met (e.g. a new exploit was discovered which renders all previously audited smart contracts vulnerable).

To protect the investors, end-users, and market integrity, we believe regulators and auditing firms could build the capacity for more rigorous response mechanisms. By observing current best practices and supporting further development of auditing processes, regulators' guidelines can contribute to safe, responsible, and sustainable innovation while effectively mitigating legal uncertainty and liability risks.

On Etherscan and Cardano tool

Etherscan is a popular blockchain explorer and analytics platform specifically designed for the Ethereum network. It uses historical cryptocurrency token price data and transactions, including transacting crypto addresses, value transferred, transaction fees, and gas prices. Transaction value also displays the total value of a cryptocurrency transaction on the day of the transaction. By relying on such information, investors, end users, auditors, regulators, and other officials can gather relevant information. Courts in the US have already relied upon the information presented on Etherscan as accurate and reliable "evidence on the record."

Further, on 13th August 2023, the Cardano Foundation launched the open beta phase of a new Cardano explorer. This is a first step towards developing an explorer that will address the needs of blockchain-native users and those of enterprises and regulatory entities interacting with blockchain. While it acts as a gateway to navigate information available on the blockchain, this explorer gathers relevant information related to native tokens, stake pools, staking lifecycle, smart contracts, and other important information. This Cardano explorer also allows individuals to compose and export a downloadable report about the activity of either stake addresses or stake pools. Reports like this one can cover various parameters and play an important role for those wishing to find, review, and authenticate certain information.

Q9: 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.

As many businesses dealing with cryptocurrencies try to meet new regulatory requirements regarding counterparty risk, they explore tools and mechanisms that may also be useful to regulatory bodies. Perhaps one of the most notable requirements is the so-called Travel Rule, relevant to nearly all cryptocurrency businesses operating in FATF jurisdictions. The Travel Rule dictates that Virtual Asset Service Providers (VASPs), such as exchanges, must identify the originators and beneficiaries of cryptocurrency transactions initiated by their users above a certain size. In cases where the counterparty of those transactions is also a VASP, the original VASP must then transmit that user information to the second VASP. Identifying transactions that meet the rule’s requirements, pulling users’ KYC information, and passing it on to the VASP counterparties once transactions are completed, VASPs often rely on specific tools. Such tools are important as gathering and passing the information on should be done while the user experience remains uninterrupted.

We observe tools like this offered by Notabene, Aegis Custody, Margin, ORS Group, and OP Labs. Notabene’s 2023 report findings underscore the outstanding complexities of Travel Rule compliance and show the ‘Lack of technical resources,’ 'legal uncertainty', and 'sunrise period effects' topping hindrances to Travel Rule adoption. Several VASPs are experiencing a lack of human resources and difficulties managing multiple data flows and integrating with various protocols, highlighting the challenge of protocol interoperability for the widespread adoption of compliance rules.

According to their study, data privacy challenges are among the most noteworthy legal concerns; it remains unclear how submitted information should be protected from unauthorized access during data submission to another VASP. To evaluate DeFi products, services, arrangements, and activities, we suggest the regulators explore existing tools and mechanisms, asses the challenges they meet, and provide further guidance on best practices.

Additionally, we would like to bring the regulators' attention to companies providing valuable data and analytics services in the cryptocurrency and blockchain space, such as Kaiko, Chainalysis, Messari, and others. They play essential roles in offering market insights, data analysis, and research tools, benefiting many stakeholders, including investors, traders, regulators, and blockchain projects.

Providing software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 70 countries, Chainalysis is a valuable blockchain data platform through which regulators can further evaluate DeFi activities. Chainalysis powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely.[12] As mentioned above, Chainalysis also provides insightful Reports and blog posts, which mitigate the misinformation and misconceptions within this ecosystem. Two most recent and notable ones are perhaps their blog posts on 1) 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking,[13] and 2) Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing.[14] The latter profoundly describes how government agencies and private sector organizations armed with the proper blockchain analysis solutions can collaborate to identify and disrupt the flow of funds. An achievement that is not easily achievable with traditional forms of value transfer. Blogpost further describes the common pitfalls in analyzing terrorist flows on blockchain, including Hamas, Hezbollah, and the Palestinian Islamic Jihad. In addition, Chainalysis specifically focuses on identifying and tracing transaction flows through service providers and the limitations thereof.

Similar cryptocurrency market data, analytics, indices, and research are provided by Kaiko, which offers businesses industrial-grade and regulatory-compliant data. Kaiko also empowers market participants with global connectivity to real-time and historical data feeds for use cases across the investment lifecycle.[15]

[12] https://www.chainalysis.com/
[13] https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/
[14] https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/
[15] https://www.kaiko.com/about-kaiko

The regulator may also be interested in learning about Messari,[16] a data aggregator that collects and organizes information on various cryptocurrencies, tokens, and blockchain projects. It provides comprehensive market metrics, including price data, trading volume, market capitalization, and historical cryptocurrency price charts. The platform offers research reports and analysis on blockchain projects, helping investors and analysts make informed decisions. It covers aspects such as project fundamentals, token economics, and team backgrounds. In addition, Messari curates news and updates related to the cryptocurrency market, offering a well-rounded view of current events and trends.

As such, Messari presents a valuable resource for the cryptocurrency industry and has become an integral component of the crypto ecosystem. Their data and analytics services contribute to greater transparency, market understanding, and informed decision-making for all participants in the crypto space. These services may be particularly important for regulators seeking to monitor and understand the activities and behaviors of market participants within the decentralized and often complex world of cryptocurrencies.

Finally, we consider oracles to be an essential mechanism that can help regulators assess DeFi products, services, and activities. An oracle, in the context of blockchains, is a vital mechanism that enables smart contracts to interact with external data sources or real-world events. This interaction is crucial because, without it, smart contracts would primarily rely on predefined conditions and user inputs only. Oracles bridge the gap between the blockchain and the outside world by providing information to smart contracts, allowing them to make automated decisions and take actions based on real-world data.

[16] https://messari.com/

According to Eric Tjorn Tjin Tai, there are three main types of oracles:[17]

1. **Automated Oracles:** These oracles are connected to automated systems or devices that can provide data without human involvement. Examples include self-driving cars that report accidents, sensors, input/output devices, and connections to websites or the internet.

2. **TTP (Trusted Third Party) Oracles:** TTP oracles involve human individuals who act as trusted intermediaries. For instance, a courier confirming the delivery of a package to a specified address is a TTP oracle. They provide information about complex real-world events that may be challenging for a smart contract to determine independently.

3. **Expert Oracles:** Expert oracles go further by offering evaluative judgments or assessments, such as determining the quality of delivered goods or assessing damage. These assessments may require the expertise of individuals like surveyors or certification agents. In the future, advanced algorithms might also fulfill this role, acting as impartial arbiters.

The use of oracles enhances data integrity within blockchain-based systems. Regulators can leverage oracles to evaluate DeFi products, services, arrangements, activities, and the individuals and entities involved. By relying on oracles, regulators can also access real-time, trustworthy information from the external world, helping them make informed decisions and ensure the compliance and fairness of DeFi systems. In his report for the European Commission, Roukny assesses DeFi from an information asymmetry perspective, proposing a regulatory focus on oracles and centralized entities in combination with voluntary compliance and public observatories.[18] Nonetheless, we firmly believe that oracles, by providing verifiable and tamper-resistant data, significantly contribute to the transparency and security of DeFi ecosystems, ultimately benefiting all stakeholders.

[17] Tjong Tjin Tai, Eric, Force Majeure and Excuses in Smart Contracts (May 4, 2018). Tilburg Private Law Working Paper Series No. 10/2018, accepted version published in European Review of Private Law 2018/6, p. 787-904., Available at SSRN: https://ssrn.com/abstract=3183637 or http://dx.doi.org/10.2139/ssrn.3183637

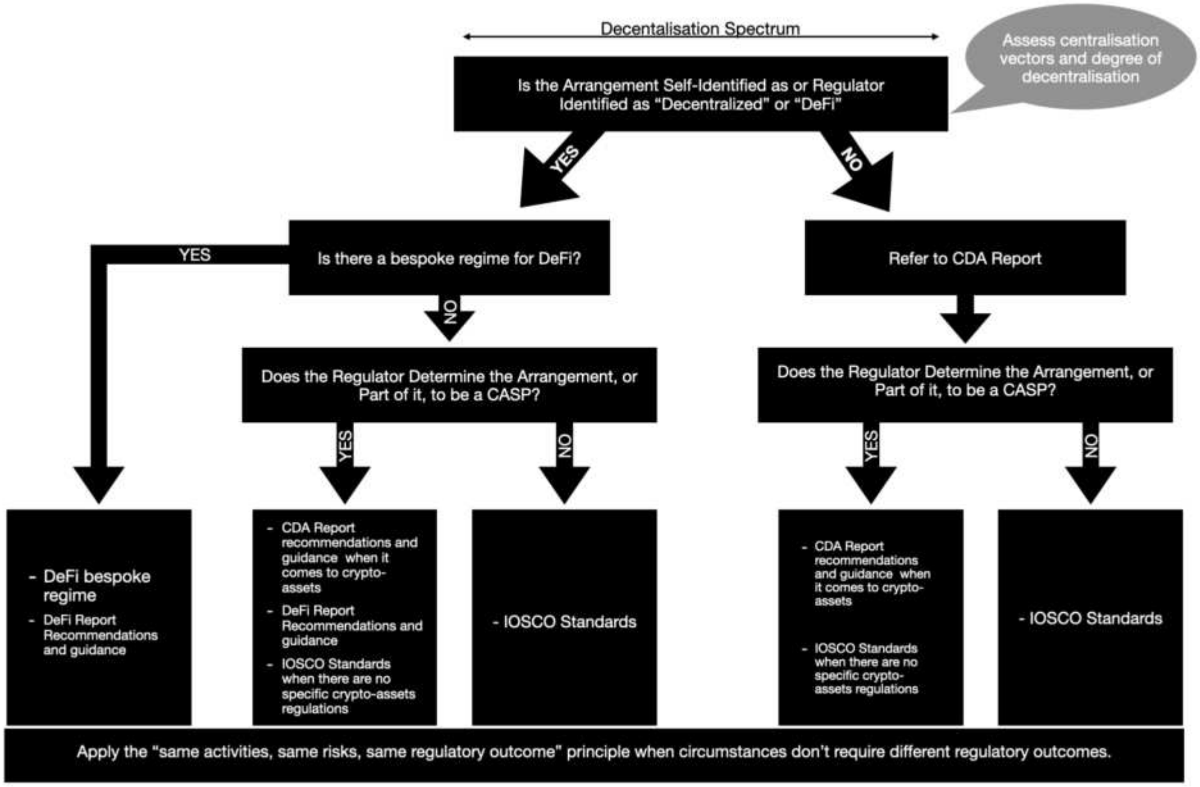
[18] Tarik Roukny, Decentralized Finance: Information Frictions and Public Policies (European Commission - Directorate-General for Financial Stability, Financial Services and Capital Market (FISMA) June 2022).

The above examples of existing methods and mechanisms showcase how the data challenges and gaps can be addressed properly. While data may be voluminous, difficult to interpret, and complex, we observe some specialized companies and organizations obtained specialized skill sets. While we agree that the information regarding asset layers, smart contracts, and applications may often be scattered and available on different platforms, the industry desires common standards. Additional guidelines on how such information is to be provided, in what form, how often it should be updated, and how addresses are disclosed properly would be welcomed by the industry as it could lead to better data flow and information sharing.

Q10: Do you find the interoperability between this report and the IOSCO CDA Report to be an effective overall framework? If not, please explain.

We consider the interoperability between these two IOSCO reports to be a highly effective development, and we welcome it, particularly in light of the recognition by regulators of the necessity for distinct regulatory frameworks tailored to specific categories of crypto assets and a separate bespoke regime for DeFi activities. These ad hoc regimes are essential, given the unique characteristics of each sector within the digital asset space.

We note 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, one that does not apply a CDA Report in situations where the regulator determines the arrangement or part of it to be a CASP, nor does it fully use IOSCO Standards in situations where specific arrangements or parts thereof are not considered to be provided by CASP. To bring more clarity towards the applicability of specific principles, recommendations, and guidance, see the proposed flow chart below:


Decentalisation Spectrum
Assess centralisation vectors and degree of decentralisation
Is the Arrangement Self-Identified as or Regulator Identified as "Decentralized" or "DeFi"
YES
NO
YES
Is there a bespoke regime for DeFi?
Refer to CDA Report
NO
Does the Regulator Determine the Arrangement, or Part of it, to be a CASP?
Does the Regulator Determine the Arrangement, or Part of it, to be a CASP?
YES
NO
YES
NO
- DeFi bespoke regime
- DeFi Report Recommendations and guidance
- CDA Report recommendations and guidance when it comes to crypto-assets
- DeFi Report Recommendations and guidance
- IOSCO Standards when there are no specific crypto-assets regulations
- IOSCO Standards
- CDA Report recommendations and guidance when it comes to crypto-assets
- IOSCO Standards when there are no specific crypto-assets regulations
- IOSCO Standards
Apply the "same activities, same risks, same regulatory outcome" principle when circumstances don't require different regulatory outcomes.

Source: IOSCO's flowchart design with the adaptions provided by the authors of this Response.

Furthermore, we appreciate the regulators' commitment to further exploring the nuanced aspects of this evolving landscape, including considerations of trade-offs, vectors of centralization, and the principles of progressive decentralization. This approach underscores the commitment to a well-informed, adaptable, and forward-thinking regulatory framework that can effectively address the complexities of the digital asset ecosystem.