October 19, 2023

International Organization of Securities Commissions
Calle Oquendo 12
28006 Madrid
Spain

SENT VIA EMAIL TO: DeFiconsultation@iosco.org

To whom it may concern,

Re: IOSCO Consultation Report: Policy Recommendations for Decentralized Finance (DeFi)

About GBBC Digital Finance (GDF)

GDF is the leading global members association advocating and accelerating the adoption of best practices for crypto and digital assets. GDF's mission is to promote and facilitate greater adoption of market standards for digital assets through the development of best practices and governance standards by convening industry, policymakers, and regulators.

GDF leads the global financial services sector as part of the Global Blockchain Business Council ("GBBC") group, the largest and leading industry association for the blockchain technology and digital assets industry with more than 500 institutional members, and 231 Ambassadors from across 109 jurisdictions and disciplines.

The input to this response has been curated through a series of member discussions and roundtables, and GDF is grateful to its members who have taken part.

The GDF also contributed to a joint industry response with the Global Financial Markets Association (GFMA) which reflects the views of GDF members within this submission, as well as those of the broader financial services industry. For consistency, we have included key aspects of the joint response within this submission as well.

As always, GDF remains at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail with our members.

Yours faithfully,

Elise Soucie
Director of Policy & Regulation, GBBC Digital Finance

Response to the Consultation Report: Executive Summary

Overall, GDF welcomes the work IOSCO is doing to bring clarity in the interest of consumer protection and market integrity, and we are supportive of IOSCO's intent of providing much needed clarity to the market. We appreciate the agility and speed with which IOSCO has aimed to develop guiding principles for the market, and we believe the report is an important step towards building a comprehensive global framework for digital assets and Decentralised Finance (DeFi). GDF is committed to continuing to work with IOSCO in meeting these aims. As such, the response to this consultation report looks to provide suggestions of areas where further precision may be needed in order for IOSCO member jurisdictions to successfully implement the nine recommendations. GDF has worked with our members to provide a constructive assessment of how to overcome challenges in implementing the recommendations and also included some technical examples of industry best practice that were highlighted over the course of member discussions. The following are the key principles discussed in further detail in our full response to this consultation:

1. The Importance of Clear Definitions

GDF believes that IOSCO should clearly define and distinguish the difference between an underlying DeFi Protocol which involves general connectivity technology or infrastructure utilising a peer-to-peer communication Protocol or network (whether involving distributed ledger technology (DLT) or otherwise) and what constitutes a "DeFi Arrangement". DeFi is a set of composable financial tools that are trust-minimised, transparent, and accessible to anybody on the internet. In order to understand what the opportunities and implications are, we must first understand the constituents that bring us to the point of consumption.

While we note IOSCO's hesitance to set out a one-size-fits-all prescriptive taxonomy, we believe that it is important to note that even a high-level definition in IOSCO's final report will have an impact on the global digital finance markets. Clear and precise foundational definitions are necessary prerequisites to achieving the outcomes sought to enhance market integrity and investor protection. Absent consistency in these fundamental definitional elements, individual regulatory structures may be premised on inconsistent underpinnings thereby challenging the objectives sought by both the regulators and the market participants offering products and services across jurisdictions. Without clarification, market participants cannot be sure whether they, or any of the activities or Arrangements in which they engage, would be in scope for the DeFi Recommendations. Additionally, some market participants may fail to develop or use beneficial technology because the definitional uncertainty underlying the DeFi Recommendations makes it difficult to understand what new or existing rules apply to it. This latter uncertainty has been an important factor that has influenced prudentially regulated firms to pause from using DLT on a more widespread basis, which both inhibits innovation and efficiency and denies market participants, including end-customers using DLT, as well as the marketplace as a whole, the safety of transacting through such firms.

GDF would suggest that the complex nature of DeFi systems necessitates a multi-factor approach to determining "decentralisation". To address these issues, IOSCO should clearly define what constitutes a "DeFi Protocol" and "DeFi Arrangement" and apply its recommendations to the use of DeFi Arrangements to provide financial services as opposed to more ambiguous phrases such as DeFi "products," "services" or "activities. Thus, any test must be based on tenets surrounding decentralisation: self-reliance for and independence over one's own transactions and for information about such transactions. Furthermore, DeFi

Protocols should be clearly delineated from any varying form of DeFi Arrangement which may be built on or interfacing with the DeFi Protocol. Given this, we would propose the following Definitions:

A **DeFi Arrangement** is a distinct financial product or service built on or interfacing with a DeFi Protocol, facilitated through technology infrastructure designed to enable end-users or investors to engage in financial transactions communicated or recorded through the DeFi Protocol.

A **Decentralised Protocol** (DeFi Protocol) is a Credibly Neutral Decentralised Network on top of which financial products and services are created. This is further expanded in Annex 1.

- **Credibly Neutral:** A verifiable and transparent system that aligns incentives with its users.
- **Decentralised Network**: A distributed, permissionless, and jurisdiction-neutral infrastructure. Its architecture inherently facilitates user autonomy, value management, and an open-source ecosystem.

These definitions are intentionally narrow. Based on this definition, there are inherently no responsible persons in a DeFi Protocol as outlined in Recommendation 2. In instances where a DeFi Arrangement claims to be 'DeFi' but is in fact centralised, we would agree with IOSCO that this type of 'DeFi Arrangement' is an entity. If such a DeFi Arrangement were to be providing regulated financial services, it should then be subject to the appropriate regulatory treatment. In cases where a business or project is built on or interfacing with the DeFi Protocol and is evolving into some form of a centralised entity, a 'sandbox' may be beneficial in order to support them developing the necessary licensing and compliance.

Overall, we would propose that decentralisation exists on a continuum. Our proposed definition of a DeFi Protocol would lie at the furthest end of decentralisation. At the other end, we support IOSCO in that where full centralisation exists, entities should be subject to the existing recommendations in the paper. Our aim with the proposed definition is to clearly delineate a DeFi Protocol (as defined above), which should be distinct from, and not be subject to Existing Frameworks or the recommendations. This is provided the DeFi Protocol is sufficiently decentralised and does not provide regulated financial services to end users, relative to business or projects (DeFi Arrangements) built on or interfacing with the DeFi Protocol. Depending on their products, services, or activities, businesses or projects may need to be subject to Existing Frameworks or New Frameworks in some form.

2. Support for an Appropriate Principles Based Approach

GDF supports the Consultation's proposed adoption of a principles-based and outcomes-focused regulatory framework for crypto-assets. A principles-based approach provides the necessary flexibility to address the diverse nature of crypto-assets, which often differ significantly in terms of technology, utility, and potential risk profiles. By avoiding rigid rules and blanket regulations, the regulators can better respond to the dynamic and rapidly evolving crypto landscape.

However, it is important when setting out principles-based recommendations to also consider under what parameters these principles will be implemented by IOSCO member jurisdictions.

Cross-border consistency is critical to prevent any unintended regulatory arbitrage and to support innovation, investor protection, market integrity, and fair practices, as well as facilitate mutual recognition between member jurisdictions.

Our responses to the questions within the Consultation suggest such parameters that could be included in IOSCO's end of year report on DeFi. We believe that providing this additional precision alongside the principles will support IOSCO in meeting its goals in this complex and rapidly evolving area of digital finance.

In order to support this, we have also proposed a flow chart showing how we propose the CDA and DeFi recommendations should apply. This can be found in **Annex 3.**

3. The Criticality of Risk Weighting

GDF also notes that IOSCO reiterated the need to take a technology neutral approach and therefore apply the principle of 'same activity, same risk, same regulatory outcome'. These are important concepts that are based on centralised control and operations commonly described as Traditional Finance (TradFi). Notwithstanding this, these concepts should and could be appropriately applied to all regulated financial products and services, irrespective of whether created on DeFi Arrangements. If we apply our proposed definition we have proposed above, there are existing projects purporting to be DeFi Arrangements that would fail the Sufficiently Decentralised and Credible Neutrality characteristics, giving rise to existing centralised touchpoints. Such entities might then be more appropriately subject to regulation (e.g., CASPs). We do not believe, however, that it would be appropriate to apply the recommendations to the DeFi Protocol itself if it meets the criteria set forth in our definition.

Further, the principle of "same activity, same risk, same regulatory outcome" often assumes an equivalence of risk across activities deemed to be the same. With respect to DeFi and digital assets however, this assumption does not adequately account for the differences due to the differences in the way DeFi products and services are delivered relative to centralised traditional financial entities (TradFi). These fundamental differences can span:

- the governance of DeFi entities involved, including decentralised governance and consensus mechanisms.
- novel technologies such as smart contracts, decentralised Protocols, settlement layers, and Dapps.
- new products and services such as aggregators and liquid staking.

Because of these critical differences between TradFi and DeFi more emphasis should be placed on conducting an appropriate risk weighting and assessing where the risk truly lies, including novel risks that are not apparent in TradFi, as set out in the annex of the Consultation. Further, we would also encourage IOSCO to define 'what' or 'whom' it seeks to regulate when addressing certain risks that may arise from the use of DeFi Protocols.

4. Best Practices for Intermediaries

With our proposed definition, financial products and services built on or interfacing with DeFi Protocols may, in some cases, be unlikely to include touch points that involve traditional centralised intermediaries. This is further discussed under question 1, recommendation 2. Yet there may be DeFi Arrangements that do involve identifiable responsible persons in some form.

In this case, we would note that GDF supports the regulation of intermediaries, as well as the "Responsible Persons" who are part of the businesses or projects carrying out financial services or some form of centralised digital asset activities. However, we would also note that there are certain actors who are not intermediaries (nor likely to be a responsible person), including (but not limited to) personal wallets, miners/validators, providers of APIs and block explorers, various types of software providers, and anything that is a DeFi Protocol (as defined). We are concerned that lack of a clear definition, as set out under point 1, would lead to the regulation of non-intermediaries and/or proposals to regulate them like financial services intermediaries. As these other categories of actors are generally not regulated in the financial services industry, we would not support their regulation in emerging DeFi frameworks.

Additionally, we believe that IOSCO should exercise caution before recommending that regulators impose requirements on the development, maintenance, or use of DeFi technology infrastructures that would require the unnecessary involvement of an intermediary. In particular, before recommending the intermediation requirements on DeFi Arrangements, IOSCO should assess alternatives, including the costs and benefits of such requirements, similar to what has been done in the swaps and other markets where central clearing or exchange trading rules have been adopted. This may include alternative methods of supervision and enforcement leveraging the DeFi technology infrastructure and ecosystem itself, as well as third-party RegTech (management of regulatory processes within the financial industry through technology) solutions.

Furthermore, we believe that the recommendations should focus on the approach which regulated entities should take when interacting with DeFi Protocols as opposed to the regulation of the DeFi Protocols themselves. Further guidance could be adopted such as Protocol level due diligence ("know your Protocol") to be conducted prior to interacting with such Arrangements and adequate disclosures to be provided to customers who are being provided access or exposure to these decentralised Protocols.

IOSCO should, in consultation with market participants, foster the development of common standards centralised intermediaries using DeFi Protocols in order to address threats to operational or market integrity and to promote retail customer protection.

Response to the Consultation Report: Questions for Public Consultation

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

GDF supports the continued efforts by IOSCO to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies for the digital asset ecosystem, including coordinating a balanced approach to decentralised finance (DeFi) across national financial authorities and international standard setters. Overall GDF welcomes the work IOSCO is doing to bring clarity in the interest of consumer protection and market integrity. We are supportive of IOSCO's intent to provide regulatory clarity and consistency to the market.

In support of these aims, we have set out the below additional suggestions for consideration as additional guidance and parameters for inclusion in the IOSCO final report alongside the recommendations. In line with these detailed recommendations below we have also included

proposed amendments to the recommendations themselves which can be found in **Annex 2** of our response.

In support of our recommendations, we would also reiterate our proposed Definitions:

A **DeFi Arrangement** is a distinct financial product or service built on or interfacing with a DeFi Protocol, facilitated through technology infrastructure designed to enable end-users or investors to engage in financial transactions communicated or recorded through the DeFi Protocol.

A **Decentralised Protocol** (DeFi Protocol) is a Credibly Neutral Decentralised Network on top of which financial products and services are created. This is further expanded in Annex 1.

- **Credibly Neutral:** A verifiable and transparent system that aligns incentives with its users.
- **Decentralised Network**: A distributed, permissionless, and jurisdiction-neutral infrastructure. Its architecture inherently facilitates user autonomy, value management, and an open-source ecosystem.

Using these definitions, it is possible to separate DeFi Protocols from the products and services built on or interfacing with them. We hope this delineation will support IOSCO in their analyses. To bring this to life more clearly, please see the following example below which we will expand and discuss further throughout our comments on the recommendations:

Example A
Consider the following hypothetical example of a project that is evolving in the DeFi ecosystem. 'ADeFiProtocol' (ADP) is a hypothetical decentralised non-custodial liquidity market Protocol. Henceforth referred to as ADP.

- *ADP is a Protocol that provides a lending infrastructure – this is the DeFi Protocol.*
- *Consider three different user interfaces[1] to the DeFi Arrangement – these are the products or services:*
  - *User Interface #1 is a command-line interface engaging with the DeFi Protocol.*
  - *User Interface #2 is a more user-friendly free interface engaging with the DeFi Protocol.*
  - *User Interface #3 is a revenue generating product that routes through its proprietary versions of smart contacts and uses the DeFi Protocol for backend operations.*
- *Regulatory touchpoints*
  - *User Interface #1 is out of scope as it is a text-based interface designed for specialized technical interactions with a DeFi Protocol. Thus, this is not a regulated financial activity or product.*
  - *User Interface #2 is a user access point for which certain risk disclaimers and disclosures may be beneficial.*

[1] A user interface's primary purpose is to generate sign requests based on user inputs, translating human-readable input into machine-readable output.

- *User Interface #3 meets the definition of a DeFi Arrangement. Thus, if it is providing a regulated financial service or product in a jurisdiction, it would be subject to an Existing or New Framework.*

Rec. 1 – We are supportive of regulators seeking to understand DeFi products and services at an 'enterprise', 'functional', and 'technical level if possible. Noting that an "enterprise" does not exist for DeFi Protocols as set out in our proposed definition above. However, we also would propose utilising our proposed definition alongside this analysis to build an understanding of the DeFi Protocol and how it is separate from a DeFi Arrangement. In order to support this analysis and clearly delineate the Protocol from the DeFi Arrangement we would encourage IOSCO to set out a clear test for assessing if the DeFi Protocol is in fact a Credibly Neutral and Sufficiently Decentralised – if it is, then it should be separate from the analysis of the DeFi Arrangement built on or interfacing with it.

If the DeFi Arrangement is not a Credibly Neutral Decentralised Protocol, then it likely lies somewhere on the continuum of DeFi Arrangements. If it is fully centralised and providing regulated financial services activities, then IOSCO members should consider the appropriate form of regulation to apply. This is a critical assessment for regulators. Please see the following example, building on Example A which further illustrates this point:

Example B
A for profit business created with a user-interface that provides money market and lending services onchain is reflective of a centralised entity that exists within TradFi. However, one difference that regulators may wish to consider is that the on-chain business uses ADP as part of its backend operations while the TradFi businesses leverage traditional infrastructure to support their operations.

Therefore, a proportionate regulatory approach to the onchain business could be similar to that which is taken in TradFi. We would note however that lending activity may be consumer credit and therefore outside of IOSCO's scope.

Regardless, the regulatory treatment should not be more or less stringent than for that of a similar business using other forms of technology unless it has been determined via the appropriate disclosures that there are blockchain-specific risks arising from ADP smart-contract risks and/or ancillary function risks like oracles. Similarly, to third-party risk management in TradFi, the DeFi Arrangement providing the service to the end user should mitigate these risks and demonstrate the risk mitigation process (if appropriate) to regulators/supervisors.

While we understand IOSCO's caution to not set out a one-size-fits-all definition given the still evolving nature of DeFi, a consistent global assessment mechanism would aid regulators in their analyses of products, services, and activities, as well as separating out DeFi Protocols from DeFi Arrangements. It would also support IOSCO's aim to promote global consistency.

Furthermore, given the reports focus on economic function rather than definition, we would also encourage the final report to include, for example, a guide to assessing whether a DeFi Protocol is Credibly Neutral and Sufficiently Decentralised. This would provide a foundational parameter through which the recommendations could be applied.

The following links provide further details on how to reference if a DeFi Protocol is a Credibly Neutral and Sufficiently Decentralised:

- Decentralized Protocols – A brief summary that can support the assessment
- Decentralized Protocols – An in depth summary to support further analysis
- Isitdecentralized.app – A website that can support testing of decentralisation

Rec. 2 – First, we would note that as discussed in the executive summary above, decentralisation exists on a continuum. A DeFi Protocol would lie at the furthest end of decentralisation. At the other end, we agree with IOSCO that where full centralisation exists, entities should be subject to Existing Framework or New Frameworks, as appropriate. For this recommendation and all that follow we would encourage IOSCO to clarify that a DeFi Protocol should not be subject to the recommendations provided they are sufficiently decentralised and do not provide regulated services to end users.

We would divide the application of Recommendation 2 into three categories supported by a further example:

1. If the DeFi Protocol fits our proposed definition and continues to do so, then regulatory focus for the application of the principle can be devoted to the DeFi Arrangement's products and services developed on top of the DeFi Protocol to find the Responsible Person.
2. If the DeFi Arrangement does not fit our proposed definition completely, but still exhibits characteristics of decentralisation then it likely lies somewhere on the continuum of DeFi Arrangements. If it is still evolving, then a 'sandbox' approach could enable the DeFi Arrangement to work cooperatively with regulators as it works towards a sufficiently decentralised end state.
3. If the DeFi Arrangement is wholly centralised, then regulators should indeed use the tools within their mandates to regulate as appropriate. We would suggest that this is not on the DeFi continuum at all, but rather an entity conducting regulated financial services activities under the pretence of DeFi without appropriate permissions and may be operating illegally or fraudulently. In this case, we support the principle in determining the responsible person within the enterprise and enforcing consistent with traditional supervisory methods.

Example C
If someone forked the ADP code and stood up another lending infrastructure, it could be a DeFi Arrangement evolving towards a sufficiently decentralised end state and could benefit from a regulatory Sandbox approach.

If the code did not result in the definition of a DeFi Arrangement, as proposed here, and the operators wished to continue promoting it themselves – then it would have a point of centralisation and the Responsible Person would continue to be those who promote it, or the Responsible Person previously identified in the sandbox.

Secondly, in traditional markets, firms are typically subject to registration or licensing requirements only if they perform some sort of intermediation function that implicates market integrity or customer protection considerations. In particular, the sort of functions that typically trigger registration or licensing typically include: discretion over the routing or execution of customer orders; access to confidential customer information; control over

customer funds; solicitation and acceptance of money for investment purposes; receipt of compensation based on effecting transactions or providing investment advice; or acting in a market making or other principal dealing capacity.

The type of technology used by a firm to perform these functions does not typically affect whether the firm triggers a registration or licensing requirement. But once a firm triggers such a requirement, its use of technology may be subject to regulation, including requirements designed to mitigate conflicts of interest and operational and technology risks and to ensure clear, accurate, and comprehensive disclosure. Importantly, in these contexts, it is the intermediary that must satisfy these requirements, not the technology developer or provider. Relatedly, the intermediary is not responsible for the use of the technology by others. So, for example, a broker who uses a vendor's order management software to route and execute its customers' orders will typically be required to take steps to mitigate the risks of using that software and provide adequate disclosure to its customers about how it handles their orders, but typically the vendor itself will not be regulated and the broker will not be responsible for use of the vendor's software by third parties.

We are concerned with the expansive framing of DeFi Recommendations 2 and. Specifically, one could read DeFi Recommendation 3 to provide for a regulator to determine whether a particular technology (*i.e.,* a DeFi product, service, Arrangement, or activity) can be used by a market participant to substitute for use of a market intermediary and then apply relevant market intermediary requirements to the Responsible Persons for that technology. Recommendation 2, in turn, appears to define "Responsible Persons" broadly to encompass persons involved with technology development or governance even if they do not themselves perform market intermediary functions (*e.g.*, requiring Protocol developers and governance token holders to register even if they do not exercise discretion over order handling, have access to confidential information, have control over funds, or receive transaction-based compensation). Thus, as framed in the Consultation Report, those Responsible Persons could have regulatory obligations with respect to uses of the technology by third parties even when they do not directly participate in such uses (*e.g.*, to prevent third parties from using the Protocols to engage in manipulative trading even if they access the Protocol wholly independently).

Such an approach would diverge significantly from what we see in TradFi markets. It would be equivalent to requiring that the order management software vendor in the example above register as a broker or perhaps an exchange (or, depending on how IOSCO defines "DeFi Arrangement," possibly to require developers of common Protocols to so register). Once registered, the person would then need to take responsibility for everyone's use of the technology, which would in turn necessitate central handling of communications transmitted using the technology. The cumulative effects of these requirements would be to prohibit use of open source or permissionless technology in financial services and instead require financial market transactions always take place through a central intermediary instead of peer-to-peer. This could have a chilling effect on innovation in financial services more broadly as invariably TradFi and DeFi are becoming interconnected to the point where financial services firms may reject technology and innovation due to concern about punitive regulatory treatment. This could ultimately impact innovative countries' competitiveness and GDP in a globally connected and increasingly digital world.

In summary, we believe the use of DLT by a DeFi Arrangement should not result in either more or less stringent regulatory treatment than other forms of technology. This is also consistent with IOSCO's stated aim of technology neutrality.

a) Consistent with existing rules and guidance, merely developing or contributing to the governance of technology should not result in registration or licensing absent some ongoing discretion over, or compensation from, transactions making use of the technology. This may include, but is not limited to, the effects a more expansive registration or licensing requirement could have on existing technology in traditional markets (e.g., communications/order management Protocols).

b) Nor should the mere use of a token as part of the operation of a DeFi Arrangement (e.g., an LP token, which acts as a receipt/ledgering mechanism for certain DeFi applications) result in the treatment of the token as a security or other financial instrument absent some use of the token for capital raising purposes or to memorialise ongoing rights and obligations vis-à-vis an issuer or counterparty.

c) Conversely, an intermediary who uses a DeFi Arrangement to provide brokerage, clearing, settlement, asset management or other regulated financial services should be subject to regulation to the same extent as an intermediary providing the same services using a different technology.

GDF also believes that IOSCO also should exercise caution before imposing requirements on the development or use of a technology that would necessitate involvement by an intermediary where one otherwise need not be involved. It may be beneficial to begin by assessing the costs and benefits of such a market structure requirement similar to what has been done in the swaps and other markets where central clearing or exchange trading rules have been adopted.

Furthermore, we support IOSCO in the principle that regulated financial products and services provided within DeFi should be appropriately regulated. There are certain actors within the DeFi ecosystem, however, who are not providers of regulated financial services and products, including those infrastructure providers involving in personal transacting and the provision of technology and data services e.g., personal wallets, miners/validators, providers of APIs and block explorers, various types of software providers, and anything that supports regulated financial products and services, as set out under our new proposed definition. These activities do not require regulation unless the principles apply to analogous activities of more traditional actors (e.g., technology companies). These actors/activities do not constitute intermediation of transactions or maintenance of custody. They are akin to internet service providers, email services, Google docs/sheets/slides and the Microsoft equivalents, web browsers, and website development and hosting providers. The terms of use for any such actors disclaim liability and regulators do not require that they obtain licenses even when financial instrument transactions flow through their services. We would not support their regulation nor efforts to regulate them like financial services intermediaries.

Another group of actors that we believe should be explicitly excluded is those engaged in peer-to-peer or peer-to-Protocol activities. Where an actor is not functioning as an intermediary but rather acting for themselves, the recommendations in the Consultation Report should not apply. Blockchain facilitates individual participant control; the use of cryptography is one of the keys to ensuring such control by requiring the user to sign each

transaction with their private key, making it impossible for a validator or personal wallet software creators (or other mere technology providers or participants) to participate in or interfere with the user's chosen activity.

Rec. 3 – Overall, GDF is supportive of IOSCO's intent to achieve common regulatory outcomes through this recommendation. But would again note, given our proposed definition of a DeFi Protocol, the regulated products and services developed on top of the technology neutral infrastructure would serve as touch points for regulators in all jurisdictions where those products and services are made available. We further expand on our example below:

Example D
If ADP is considered a DeFi Protocol, then any for-profit business built on or interfacing with it that is providing regulated financial products or services would be accountable to the appropriate jurisdictional framework for those products and services in the regions where it wishes to operate. On the other hand, the current user interface of the DeFi Protocol itself which is a free accessible user interface (User Interface #2) is a user access point for which certain risk disclaimers and disclosures may be beneficial.

Furthermore, we would also expand on this example to note that the mapping set out in this recommendation relies on centralisation. Given our proposed definition of DeFi Protocol we propose to delineate those arrangements which have centralised regulatory touchpoints from the technology neutral Protocol. Referencing our above example, if ADP meets our proposed definition of a DeFi Protocol, the infrastructure of the DeFi Protocol may provide the capability to construct pools, but the DeFi Protocol does not otherwise have custody of or manage the pools.

We would, however, recommend caution that in aiming to apply existing regulation, that jurisdictions implementing this principle do not inadvertently fail to contemplate risk weighting. Risk weighting is influenced by both the likelihood and consequences of a risk occurring and, if it does occur, what the consequences would be. This analysis is crucial to determining responsive preventative and detective risk mitigation measures.[2] Thus regulators must work to understand the distinction between DLT, the technology, the use cases built on or interfacing with it (and what use cases are being employed in any DeFi context), and the risks (higher or lower) that then may be posed by in that specific DeFi Arrangement. Regulators can then determine if their existing framework is applicable, and if not, what innovative solutions can be developed to regulate DeFi in order to align to the functionality of the different roles occurring within the DeFi ecosystem with TradFi. This is also in alignment with IOSCO's stated approach set out under Recommendation 1, noting the importance of analysis, and understanding of DeFi at both an 'enterprise' and functional level.

Like a traditional database model, there are ways to develop DeFi Arrangements to be more controlled—not only to comply with existing regulation but also to make such compliance more seamless, comprehensive, and effective.

Additionally, we would note that it is not yet clear whether *all* DeFi activities (noting the lack of clarity in definitions globally) would meet the definition of financial instruments set out under recommendation 3. As legal and regulatory frameworks continue to evolve, it is

[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), Available at SSRN: https://ssrn.com/abstract=4571106

important for IOSCO to consider how their principles can be future proofed to these developments.

Rec. 4 – GDF is supportive of the aim of this recommendation and agrees that it is important to both identify and address conflict of interest in a way that meets the high standards of regulated financial markets. As discussed under the previous recommendations, if it is a DeFi Protocol then the focus should be on the Responsible Persons operating products and services built on or interfacing with the technology neutral infrastructure to avoid conflicts of interest. For example, the Responsible Persons who contribute to the DeFi Arrangement, rather than the Protocol, and run a service on top of it would naturally fall into this category. If it is not a DeFi Protocol, then regulators should seek to determine where it falls on the continuum of decentralisation as set out under Rec. 2 above and apply an appropriate regulatory approach accordingly.

To further delineate this point, we would also caution that for a DeFi Protocol there may *not* be conflict of interest or indeed any relationship at all between the technology neutral infrastructure layer and/or application and user interface layer either because it is fully automated or is operated as fully decentralised with fully decentralised infrastructure and governance. In this instance, to mis-identify a Responsible Person at the layer of the infrastructure may inadvertently hold as liable uncoordinated actors such as developers, Protocol governors, DLT network validators, internet service providers, digital asset creators, liquidity providers, IT service providers, and many others.

For example, DeFi Arrangements may leverage usage-neutral software as a component of a system that brings together buyers and sellers of securities. Such arrangements may also be used for bringing together counterparties to non-securities transactions such as event tickets or collectibles. The software component utilized by a decentralised financial system may not even be constrained to use in an exchange environment. However, recommendations 2 and 4 may potentially capture the developer of the software component (the DeFi Protocol) as liable or responsible if the component is later used to provide services to an end user, even if the software is used under an open-source license. In addition, DeFi Protocols may be operated by usage-neutral infrastructure providers, such as internet service providers or public DLT network validators. The proposal does not meaningfully distinguish which infrastructure providers may be captured 'as responsible' if their infrastructure is later used to provide regulated activities to an end user.

Given this potential for inadvertent liability, which would counter IOSCO's intent of technology neutrality, we would support additional parameters, such as those included in our proposed definition, that link back to recommendation 1, to create greater specificity in the application of IOSCO principles where the responsibility is with those who are providing regulated financial services or activities within IOSCO's defined scope of responsibilities. We agree with IOSCO that where there is indeed conflict of interest and the base layer is integrated with the user interface, then all those involved in the regulated 'enterprise' should be held liable. But it is important to make a clear distinction where this is not the case in order to avoid stifling innovation, and mis-identifying those in conflict or responsible.

Rec. 5 – GDF is supportive of the overall principle of this recommendation. We agree that to develop a robust digital finance ecosystem it is imperative to identify and address material risks. As discussed under the above recommendations, assuming such providers and responsible persons can be identified then traditional rules relating to operational resilience

and risk management would apply. Clarifying this definition is important. For example, a statement such as, "[a] provider of DeFi products and services often has control over the smart contracts incorporated into the product or service," could create confusion as to what a DeFi Arrangement actually is, since a DeFi protocol is not decentralized if a single entity retains control over its smart contracts. This may, however, occur for a DeFi Arrangement evolving towards a sufficiently decentralized end state, in which case a sandbox approach is recommended. Otherwise, it is a project purporting to be a DeFi Arrangement where in fact it's more likely to be a centralised entity carrying on regulated financial services or activities.

To further expand on this point, it is one of the innate challenges of DeFi that DeFi Arrangements may be built leveraging the usage-neutral software of DeFi Protocols involving a range of autonomous and globally dispersed developers. If it is a DeFi Protocol, a software provider in one layer of the DeFi stack, will not have individual control of open-source software or smart contracts in another layer. Those smart contracts are able to be copied and reused in a composable fashion to create new products and services 'Lego style'.

It is therefore possible that software built for one purpose on chain, can be reused for another purpose different from what was intended when originally uploaded. While we are broadly supportive of the overarching principle of recommendation 5 it is important for regulators to consider how DeFi service providers and their relationship with the underlying software (and DeFi Protocols) may differ greatly from a traditional financial markets third-party provider relationship.

Given that (1) DeFi node operators are inherently decentralised with no specific jurisdictional location, (2) contracts are visible to all and can be edited, and (3) a smart contract deployer has no control over the contract's subsequent use, we believe regulators should instead look to the most centralised point in the chain: business offering to the end user of the regulated financial service when determining how to assess and address material risks. Although challenging and requiring new ways of working, this may be the most effective avenue for regulators to operate in the decentralised space. This is also applicable to the following IOSCO recommendation 6 on disclosures.

One additional suggestion in relation to oracles as set out in the box under recommendation 5 is to evaluate oracle risks by confirming if it is an on-chain oracle. If it is on-chain, then risks should contemplate how the respective data feeds are aggregated (e.g., for prices, does it include a TWAP (Time Weighted Average Price)). If it is an off-chain oracle, then risks reviewed should focus on risks related to the specific oracle as well as the number of nodes, etc.

Rec 6. – GDF is supportive of this principle, taking into account the constraints that may exist as set out under the other recommendations above. We note that our proposed definitions will also facilitate the identification of touchpoints for appropriate reporting and separate DeFi Protocols from DeFi Arrangements.

We would also encourage regulators to continue to cooperate and work with industry to develop these innovative solutions. One example of this is set out in a recent paper by Chris Brummer, which details how, "DeFi presents novel policy questions for disclosure because much of the material information required to participate in an informed way is already available to technologically sophisticated actors on blockchains… The paper offers a

framework for revamping Regulation S-K [and] emphasises the need for shorter, crisper disclosure approaches typically associated with consumer protection law. Highlighting the point, the paper additionally draws attention to the necessity of clarity and "Plain English" in disclosures for not just the business, but also technology in the space."[3]

Rec 7. – GDF is supportive of this recommendation and believes it is crucial for DeFi to be appropriately included in emerging regulatory frameworks in order to support the development of a robust, viable, and transparent digital assets ecosystem.

Utilising the new proposed definition, regulators would be able to conduct an appropriate assessment of what is a DeFi Protocol, and what is a DeFi Arrangement and what regulated financial services are being provided to end users. If there are points of centralisation which provide regulatory touchpoints in the DeFi Arrangement, we would support the use and application of regulatory tools within their emerging and existing frameworks.

We would, however, also reiterate our suggestion under recommendation 3 that the appropriate risk weighting and risk assessment be included in the application of relevant laws. GDF would also re-emphasise that it is equally important to draw precise boundaries around actors and activities that are not covered by regulatory obligations or liable for regulatory compliance. In supporting IOSCO's aim of being technology neutral, this precision is necessary in order to prevent the unintended consequence of valid regulatory concerns resulting in an overexpansion of regulatory obligations and compliance liabilities from primary actors who *do* provide regulated services to end users, to "facilitators" (or other similarly broad categories of actors who *do not* provide services to an end user) to account for the decentralised nature of digital asset infrastructure.

Furthermore, we support continued efforts by regulators to continue to collaborate and consider how to upskill together. It is crucial for the regulatory community to also explore creative solutions for their own internal processes, as traditional tools may be challenging to implement for the most effective DeFi regulatory solutions.

Rec 8. – GDF is fully supportive of this recommendation and believes it is of the utmost importance in order to create a comprehensive regulatory framework for digital assets and prevent regulatory arbitrage. However, we would also suggest adding to the areas set out a comprehensive cross-border taxonomy for digital assets. This is important in order to mitigate any unintended cross-communication between jurisdictions and will also provide much needed regulatory clarity for the market. Additionally, in order to have robust and consistent cross-border enforcement, agreement of key terms and legal Definitions will be needed.

Furthermore, we would note it is important for IOSCO to consider how IOSCO members would apply the principles with respect to mutual recognition. Recommendation 8 explicitly discusses cross border cooperation and information sharing but does not contemplate the application of mutual recognition across jurisdictions may be an acceptable approach to the regulation of borderless fintech services.

We would note that DeFi, by its decentralised nature, operates in a jurisdiction neutral manner. Yet, the recommendation does not address the inherent challenges posed by DeFi's

[3] Brummer, Christopher J., Disclosure, Dapps and DeFi (March 24, 2022). Forthcoming, Stanford Journal of Blockchain Law and Policy, Available at SSRN: https://ssrn.com/abstract=4065143

global reach. It omits the vital necessity of mutual recognition in regulatory approaches – an approach which would create enhanced efficiency for a global regulatory framework. IOSCO could play a valuable and integral role with Recommendation 8 if it focused on the characteristics of jurisdictional approaches that would merit mutual recognition.

Rec 9. – We are supportive of this recommendation and believe it will be instrumental in supporting financial stability and mitigating any knock-on-impacts to the traditional financial services sector. This recommendation may come with unique challenges for jurisdictional implementation, and GDF remains a collaborative partner to IOSCO and its members to support them in their ongoing efforts.

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.

GDF is supportive of these efforts by IOSCO to detail some of the vast products, services, and activities that exist in the DeFi space. However, we would reiterate our proposed approach that it is crucial to first clearly define DeFi in order to separate DeFi Protocols and technology neutral infrastructure from centralised entities or enterprises that may soon be centralised, or in some unregulated or fraudulent enterprises.

We would, again, note our proposed definitions as set forth above.

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

First, we would note that it would be beneficial for the report to set out a clearer and narrower definition of governance. As with the definition of DeFi, we are concerned that too broad a definition of governance would inadvertently conflate DeFi Protocols and technology neutral infrastructure with the governance processes that occur in centralised entities. As set out previously, we would encourage further clarity and delineation in this regard.

GDF would propose a definition of governance that aligns with the below framing from Polygon Labs:

"Governance and administration relates to the authority over the functioning of the code, and by extension, potentially over third party user assets that are supplied to or otherwise used in the Protocol: (a) is there an administrative key that allows for control of the Protocol and if so, does an identifiable natural person or entity (or group of persons who know each other and intentionally coordinate with each other) hold the key; and (b) is there a central decision-making authority that can control the Protocol through governance votes or otherwise?

One key issue that is frequently overlooked in assessing governance – even in the face of certain actors purportedly having outsized "voting influence" in distributed governance systems, such as decentralised autonomous organisations ("DAOs") – is whether users ultimately have control over their assets regardless of governance votes. Even if a DAO makes changes or updates a DeFi Protocol, users should be able to (i) receive information about the changes to the Protocol in a timely manner; and (ii) make decisions about removing or otherwise changing the configuration of their assets prior to such changes taking place such that any change by the DAO would not affect user assets."[4]

[4] https://assets-global.website-files.com/637359c81e22b715cec245ad/644fc3d2c4a4b1a1cba05110_Polygon%20Labs%20-%20Response%20to%20Cryptoasset%20%20Consultation%20.pdf (Page 8)

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?

As discussed throughout our response, it is first important to delineate DeFi Protocols from the entity or operation built on or interfacing with the Protocol. If regulated financial services activities are being conducted through a centralised organisation, then IOSCO should indeed consider where it lies on the continuum of decentralisation and how it can meet the appropriate standards, regulations and principles set out in the Consultation.

Yet we would also note that code in general, not just code specific to DLT or blockchain can and does develop as open source. In these instances, liability is challenging to define and allocate. Additionally, there are methods for risk mitigation used by open-source systems who operate and are used widely across other sectors and industries beyond financial services. For example, Mozilla, Linux, Apache, and Java programming all utilise open-source solutions. Regulators should consider how to work with regulated entities to mitigate risks to end consumers, not hamper innovation by imposing requirements on the developers of the underlying technology infrastructure or software.

Separately to the above points noted above, we also highlight some best practice on risk management from Polygon Labs included in their response to the UK's consultation and Consultation and Call for Evidence on the "Future Financial Services Regulatory Regime for Cryptoassets" earlier this year.

First, "truly decentralised DeFi Protocols can be accessed primarily through self-hosted wallets – which are pseudonymous and do not provide what is typically thought of as "personally identifiable information" (e.g., name, email, IP address, etc.). "Front end interfaces" (also called "user interfaces" or "front ends") that simplify access to DeFi Protocols using those wallets do not necessarily collect information relating to IP addresses (another way to identify the location of a user); further, some front ends are hosted via decentralised systems for hosting and sharing data (e.g., the Interplanetary File System ("IPFS")), which do not allow for collecting IP addresses. In many instances, there are dozens of front ends or other access points to DeFi Protocols making it virtually impossible to track and obtain users' identities, IP addresses, or locations. Furthermore, users can access DeFi Protocols directly on a blockchain network, without the use of any front end or a centralised access point, making it impossible to know their locations."[5]

Given this, for a DeFi Protocol, "risk to users and to market integrity is borne primarily from technology and cyber risks, or the risks of integration with centralised systems (e.g., centrally issued tokens or centralised information systems such as oracles)."[6]

"To mitigate both technology and cyber risk before a Protocol is deployed, "best practice" includes robust auditing procedures – both internal and external to the development team.

---

[5] https://assets-global.website-files.com/637359c81e22b715cec245ad/644fc3d2c4a4b1a1cba05110_Polygon%20Labs%20-%20Response%20to%20Cryptoasset%20%20Consultation%20.pdf (Page 6)

[6] https://assets-global.website-files.com/637359c81e22b715cec245ad/644fc3d2c4a4b1a1cba05110_Polygon%20Labs%20-%20Response%20to%20Cryptoasset%20%20Consultation%20.pdf (Page 6)

After code is written, it should be shared with other members of the internal team who did not write the code to review to find "bugs" or other vulnerabilities (including economic and technical); then the code should undergo auditing by a third party auditor who likewise vets and tests the code to determine any flaws; and then the software development team should consider the results of any outside audit and determine whether alterations to the code are necessary to ensure proper functioning. It is well-recognised by industry that code audits are critical to ensuring safe and effective operation of a DeFi Protocol.

Third-party auditors play an important role in the safety and soundness of DeFi Protocols; there are a number of reputable, well-known third-party auditors as well as smaller auditors, all of whom could play into the possibility of self-regulatory organisations (SROs) within the context of decentralised technology.

Despite the benefits of auditing, there are at least three helpful improvements in auditing practices that can be made: first, a standardisation of the approach to auditing smart contracts for DeFi Protocols; second, a standardisation of when and how third party audits are used – e.g., prior to launch, at the time of an upgrade to the code, etc; and third, standardising transparency around Protocol audits will enhance accountability both for auditors and development teams, and will allow for even greater examination of the safety of code.

In addition, to mitigate cyber risk for Protocols not yet deployed, developers can implement "gated" or "guarded" launches, which can be done in two ways: where the developer can restrict the Protocol by limiting either the liquidity that can initially be injected into the system or the level of decentralisation for a limited time so quick updates can be implemented, or by restricting individual wallets by limiting the liquidity that a single wallet can contribute to the system.

Additional best practices for ensuring the safety of the code include, but are not limited to, bug bounty programs and 'audit competitions'. The former refers to programs where a software developer or a DAO offers rewards to individuals who find previously undetected vulnerabilities in the code and privately disclose those vulnerabilities to the developer for correction. The latter refers to events where software developers offer rewards during a specific time to a specified (frequently identifiable) group of individuals who compete to find vulnerabilities in the code for correction before deployment of a Protocol.

Finally, while not yet codified as a "best practice" or "industry standard", meaningful progress has been made with automated, technology-based monitoring systems for cyber risks. Such monitoring allows for the identification of suspicious on-chain activity, and triggers an emergency pause on the platform.

As with all parts of the DeFi ecosystem, the risk mitigation and monitoring tools continue to improve, such that current 'best practices' outlined above are not comprehensive and will evolve over time. Accordingly, any contemplated regulation should be enacted with 'regulatory outcomes' in mind rather than prescriptive requirements."[7]

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

[7] https://assets-global.website-files.com/637359c81e22b715cec245ad/644fc3d2c4a4b1a1cba05110_Polygon%20Labs%20-%20Response%20to%20Cryptoasset%20%20Consultation%20.pdf (Pages 11-12)

through the use of technology? How would you suggest IOSCO members address data gaps and challenges?

While there are challenges to regulating DeFi, there are also many emerging solutions that could support IOSCO members in addressing these challenges. Within the Consultation IOSCO set out three main challenges. We aim to offer support to IOSCO in addressing these and would provide the below feedback as a first step in mitigating some of the risks presented.

First, IOSCO noted that it is difficult to acquire skills and infrastructure needed to gather and analyse on-chain data. While we agree that the necessary technical skills and knowledge is important and appreciate the difficulties faced, we would propose that there are tools the public sector can use such as blockchain analytics or direct engagement with industry. This would also be consistent with the strategies IOSCO set out for obtaining information throughout the report.

Secondly, IOSCO discussed the challenge of lack of standardisation within the data. We believe that on this point it would be beneficial to further delineate the types of standardisation which would be recommended in order to support supervision and policy developments. The tools set out under the first challenge could also support this.

Thirdly, IOSCO raises the challenge of pseudonymity and off-chain activity. First, for pseudonymity, we recommend identifying the specific obstacles related to this. For example, we appreciate that IOSCO has an interest in "levels of retail investor participation" but this should be balanced with support for the privacy rights of retail consumers (*e.g.,* under the EU General Data Protection Regulation). For identifying and tracking illicit funds, there are blockchain-native solutions that regulators can engage with to identify specific individuals or entities (for example, through working with entities such as TRM labs). Overall, we believe there are solutions to this challenge that exist in the market, but it is crucial to clearly identify the problem and/or risk in order to come up with a precise, effective, and sustainable solution. In relation to off-chain activity, this typically involves points of centralisation, which as discussed throughout the response would not fall under our proposed definition of a DeFi Protocol, so can be regulated via existing tools that in existing regulatory frameworks.

Finally, we would suggest, as an overarching approach, further work in 2024 to promote bottom-up collaboration between IOSCO members and industry. As Eric Hess underscores in his recent paper, “Public-private collaborations can be pursued expeditiously, without waiting for digital assets legislation to be enacted, to gain early and meaningful insights that can help refine untested laws and improve their implementation.”[8] This echoes our belief in the need for regulatory clarity among DeFi stakeholders and emphasizes the cooperative approach that could foster tools for a hybrid ecosystem of both permissioned and permissionless finance models. These tools are key to enabling diverse use cases that are crucial for the industry’s success.

In addition to this overarching approach, some practical steps that could mitigate some of these the challenges include:

- A decentralised oracle certification system, with a particular focus on the consensus mechanism leading to the final result (i.e., responsible for the weighting of various data sources); and

[8] Hess, *supra* note 2, at 44.

- A circuit breaker on the provision of data from oracles.

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?

Yes, GDF is supportive of the application of IOSCO standards and principles to DeFi in a manner that reflects the differences inherent in DeFi relative to TradFi and the scope of responsibilities that IOSCO has. We appreciate the agility and speed with which IOSCO has aimed to develop guiding principles for the market, and believe the report is an important step towards building a comprehensive global framework for digital assets and DeFi.

We would encourage, following the report at the close of 2023 that IOSCO continue to work with industry to consider how the IOSCO Standards can apply, and that collaboration continues as the market continues to evolve. In such a rapidly developing area of digital finance it is crucial that IOSCO remains agile and steadfast in their support of responsible innovation, while still mitigating risks to financial markets and consumers.

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

GDF is supportive of the development of a public-private sector working group in 2024, following the completion of the IOSCO 2023 report. Given that this area of the industry is still rapidly developing, we believe that this Consultation marks an important first step towards the development of appropriate DeFi standards and regulation.

While we support, and appreciate, the need to deliver recommendations at speed to provide clarity to the market, it is also imperative to continue to support the common standards and responsible innovation that is occurring across the market.

A join public sector-industry collaboration would provide a channel through which to approach the unique challenges of DeFi, while also supporting and proliferating common standards. It is important to also include in this collaboration other sectors of industry who are integral to the infrastructure such as technology providers and technology standard setting bodies. Separately, we would also encourage IOSCO to provide further guidance on the application of IOSCO principles as regulatory frameworks around the world continue to evolve.

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.

Emerging technologies in DeFi present regulators with effective tools to support innovation while maintaining market integrity. These include 'Know Your Transaction' analytics and zero-knowledge proof queries against verified credential databases, which are designed to facilitate compliance with AML and CFT regulatory frameworks.[9] The reluctance of traditional financial institutions to engage with DeFi often stems from uncertainties around regulatory exposure, particularly in relation to AML/CFT compliance. These technologies can help mitigate such risks, laying the groundwork for future public-private collaborations that refine and improve regulatory strategies.

[9] See Hess, *supra* note 1, at 51-58.

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.

An effective strategy for regulators could be the adoption of a bottom-up approach, which would involve working closely with DeFi stakeholders to create sustainable policies and practices. An immediate action could be to hire industry experts, ensuring that those evaluating DeFi Arrangements and Protocols have an in-depth understanding of the underlying technology and its complexities.

Moreover, the formation of cross-stakeholder working groups can expedite the adaptation of existing regulatory guidance to develop common standards, particularly in areas of risk management. [10] The endorsement and transparent disclosure of such standards could further contribute to a DeFi ecosystem that safeguards both investors and market integrity.

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

Yes, GDF finds the interoperability between the two reports helpful and supports regulatory efforts to create a cohesive and comprehensive global framework.

ANNEX 1: Characteristics of a DeFi Protocol & Expanded Importance of Clear Definitions

In addition to the definition set out in our response, we recommend considering defining a "DeFi Protocol" to mean a technology that has the additional following characteristics:

- *Publicly Distributed* – the technology is hosted using public DLT or other ledger technology maintained by a group of unaffiliated parties;
- *Permissionless* – the technology can be accessed without permissioning by a party other than the user;
- *Store/record of value* – the technology is designed to manage authoritative records of asset ownership;
- *User autonomy* – users can interact with the technology without surrendering control over their assets or transactions to a third party;
- *Verifiable* – the technology provides a verifiable record of transactions and ownership;
- *Impartial* – all users of the services or products have the same rights to access the technology's functionalities;
- *Transparent* – material information about how the technology functions, how it was developed (including any testing or audits), how it is governed, and any material developer or governance conflicts of interest is publicly available; and
- *Aligned incentives* – the operation and governance of the technology is reasonably designed to align governance incentives with user incentives.

We in turn recommend defining a "DeFi Arrangement" to mean a website or other financial infrastructure created on or with a Decentralised Protocol, on top of which financial products and services are created. It may be designed for use by end-customers/investors to engage in transactions involving financial instruments communicated or recorded through a DeFi Protocol or network.

[10] See Hess, *supra* note 1, at 59-70.

These definitions have three principal goals:

First, our proposed DeFi Protocol definition is intended to functionally distinguish decentralised from centralised Protocols. In our view, the combination of characteristics set out above would largely eliminate or at least substantially mitigate the risks that the developers of the Protocol or parties taking part in its governance could, or have reasonable incentives to, abuse information asymmetries or control over the Protocol in a manner that could harm or otherwise disadvantage users. If a Protocol did not satisfy these characteristics (i.e., was more centralised in its design, and enabled users to access regulated financial services), then the party or parties responsible for developing, deploying and/or governing the Protocol should be subject to the appropriate regulation like any other financial services provider (although, in some jurisdictions, they may qualify for a regulatory sandbox or similar safe harbor).

Second, our proposed DeFi Protocol definition is intended to distinguish the use of public DLT-based Protocols from part of a firm's internal books and records or as a courtesy ledger that does not reflect authoritative records of asset ownership. Regulated financial institutions should not be prevented or discouraged from exploring, developing, and using internal, private, permissioned blockchain or a DLT-based books and records system. Further, the assets recorded on such a system (Book Entry Tokens) should not be considered financial instruments (*i.e.*, tokenised assets, crypto-assets, or digital assets); rather, Book Entry Tokens would merely represent a financial institution's book entries—for example, representing a record of, in the case of cash, the financial institution's deposit liability to its customers, and in the case of securities and other non-cash assets, the financial institutions' custody of those assets for its customers' benefit. Such recordkeeping does not affect the legal properties, risks, or other characteristics of the assets. Furthermore, Book Entry Tokens are limited to use within a firm's internal systems, have no intrinsic value and would have no value or meaning outside of the firm's books and records. For these reasons, Book Entry Tokens pose no additional risks and should be subject only to existing regulations governing internal books and records.

Finally, by separately defining DeFi Protocol vs. DeFi Arrangement, we have sought to distinguish the different layers of the technology ecosystem in order to better tailor the potential application of regulatory requirements. In particular, we think it is important to distinguish (i) general connectivity technology or infrastructure utilising a peer-to-peer communication network or Protocol (whether involving DLT or otherwise) versus (ii) a user-facing website or other application designed for use by end-customers/investors to engage in transactions involving financial instruments communicated or recorded through a DeFi Protocol or network.

The former category would generally encompass underlying public blockchains, whether a "layer 1" blockchain acting as a base-level ledger for validating and recording data or a "layer 2" blockchain that provides a scaling solution on the underlying layer 1 blockchain to make processing more efficient. These networks are typically asset or content agnostic and are more akin to the networks of routers, servers, and core Internet infrastructure.

The former category would also generally include smart contracts and other DeFi Protocols, as well as oracles and bridges, which provide rules or connectivity for parties to interact with each other over public blockchains. These Protocols are akin to common Protocols for

transferring information over the Internet, such as TCP/IP, HTTP, SMTP, and FTP. Similar Protocols also exist within traditional financial services, such as the FIX communication Protocol. In each case the Protocol is essentially just a set of common standards and specifications for sending and receiving messages and other information.

The latter category would generally include websites and applications (including application programming interfaces and certain (but not all) wallets) that enable end-customers/investors to access the underlying Protocol or network. Where they are designed to facilitate transactions in financial instruments, these applications are akin to the websites, trading systems and other applications that market participants use today to trade, clear, and settle securities and derivatives transactions through connections to underlying Internet or other telecommunications infrastructure.

Applying the DeFi Recommendations to the former category (networks or Protocols) would present a number of significant challenges, similar to the challenges that would apply if similar requirements applied to core Internet network infrastructure and communications Protocols. Most notably, when a Protocol or network is truly open source in nature and does not have a central administrator or one or more parties that act to control the network or Protocol, it lacks the element of centralised governance that can be responsive to traditional regulatory compliance requirements. Relatedly, despite efforts at harmonisation, regulation remains specific to particular jurisdictions and particular financial instruments, which again is inconsistent with open source or permissionless networks or DeFi Protocols that can be used or accessed across borders and categories of financial instruments. So, applying the DeFi Recommendations to networks or Protocols would in practice prevent development or use of open source or permissionless networks and Protocols, which would unnecessarily harm innovation and efficiency in financial services but also other interconnected industries more generally. Also, given that financial services regulation generally does not apply at the level of Internet network infrastructure or communications Protocols, applying those requirements to DLT-based networks or Protocols would violate technology neutrality.
Conversely, it also would not be technology neutral to excuse user-facing applications from financial services regulation merely because those applications connect to DLT-based networks or Protocols as opposed to networks or Protocols not involving DLT.

These concepts are also further discussed in the 2022 GBBC Digital Finance Report, DeFi: Moving the Dialogue on Standards and Regulation Forward.[11] The report outlines the key constituents of the DeFi ecosystem, summarizes the risks identified by regulatory and policy agencies, and proposes a two-track approach to moving the industry-regulatory dialogue forward:

Track 1 – Short-Term Industry Transition: Industry Standards
In the absence of regulation specific to DeFi, the industry must coordinate to establish governance and investor protection standards, as well as industry-led monitoring to demonstrate that it can operate to high standards of trust and predictability.

This could be in coordination with IOSCO members to further embed IOSCO Principles appropriately across industry but should include other cross-industry non-financial participants necessary for the innovation in the DeFi ecosystem to grow and mature responsibly.

[11] https://www.gdf.io/wp-content/uploads/2022/07/DeFi-Report_26.07.22.pdf

Track 2 – Medium to Long-Term: A Co-Regulatory Model
Industry and agencies should collaborate in a co-regulatory model to carry out the process of risk identification across the ecosystem in a shared engagement platform. This will accelerate the development of right-size regulation that is harmonized at a global level. In doing so, stakeholders have the opportunity to explore the design and operation of regulatory nodes.

ANNEX 2: Proposed Revisions to Recommendations

Please note the original text is in blue with our proposed revisions in red.

Recommendation 1 (Analyze Use of DeFi ~~Products, Services,~~ Arrangements~~, and Activities~~ to ~~Assess Regulatory Responses~~ Provide Financial Services): A regulator should assess whether particular technologies qualify as DeFi protocols or DeFi arrangements, analyze the use of DeFi ~~products, services,~~ arrangements, ~~and activities~~ to provide financial services occurring or located within its jurisdiction with a view to applying its Existing Framework or New Framework, as appropriate, in accordance with the principle of "same activity, same risk, same regulatory outcome." To do so, a regulator should aim to achieve a holistic and comprehensive understanding of such use of DeFi ~~products, services,~~ arrangements~~, and activities~~, including through consultation with DeFi stakeholders. A regulator should assess what technological knowledge, data, and tools the regulator needs to understand, and analyze such use of DeFi ~~products, services,~~ arrangements~~, and activities~~ to inform regulatory responses.

Recommendation 2 (Identify Responsible Persons): A regulator should aim to identify the natural persons and entities ~~of a purported~~ who use a DeFi arrangement ~~or activity that could be~~ to provide financial services subject to its applicable regulatory framework (Responsible Person(s). In doing so, a regulator should act in a manner consistent with its existing rules and guidance to ensure a technology-neutral approach to licensing and registration requirements for Responsible Persons. These Responsible Person(s) may include, based on the relevant facts and circumstances, those exercising control or sufficient influence over a DeFi arrangement through ongoing discretionary authority over, or receiving compensation based on, transactions making use of a DeFi arrangement ~~or activity~~. Responsible Persons should exclude those persons or entities not directly involved in providing the regulated financial service or activity, but who are involved in developing, maintaining, or contributing to the governance, or technology infrastructures of, a DeFi arrangement.

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 financial services provided through use of DeFi ~~products, services,~~ arrangements, ~~and activities~~ in a manner consistent with IOSCO Standards. The regulatory approach should be functionally based to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets. Where DeFi arrangements are used (i) in connection with traditional financial instruments or (ii) by traditional financial market service providers, a regulator should take a technology neutral approach (i.e., an approach that focuses on activities and risks conducted or posed by use of technology, not the technology itself) and apply existing frameworks wherever possible.

Recommendation 4 (Require Identification and Addressing of Conflicts of Interest): In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of regulated financial services using DeFi ~~products and services and other Responsible Persons, as appropriate~~ arrangements 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 by the providers of regulated financial services using DeFi arrangements and supervised by the regulator of such financial services provider. For example, in circumstances, such as where a provider of financial services using a DeFi arrangement also exercises self-regulatory organization authority, a ~~A~~ regulator could ~~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.

Recommendation 5 (Require Identification and Addressing of Material Risks, Including Operational and Technology Risks): In applying Existing Frameworks or New Frameworks, a regulator should seek to require providers of regulated financial services using DeFi ~~products and services and other Responsible Persons, as appropriate,~~ arrangements to identify and address material risks, including operational and technology risks. These risks should be identified and effectively managed and mitigated by such regulated financial services providers and supervised by its regulator. Only in exceptional circumstances should a ~~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.

Recommendation 6 (Require Clear, Accurate, and Comprehensive Disclosures): In applying Existing Frameworks or New Frameworks, a regulator should seek to require regulated financial services providers ~~of~~ using DeFi ~~products and services and other Responsible Persons, as appropriate~~ arrangements 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. Consistent with the approach taken in traditional financial markets, the extent and nature of such disclosures should take into account relevant market characteristics and may be tailored to the technology and particular type of users and investors (for example, whether the disclosure is to a retail or institutional user or investor).

Recommendation 7 (Enforce Applicable Laws): A regulator should apply comprehensive authorization, inspection, investigation, surveillance, and enforcement powers, consistent with its mandate, to regulated financial services providers using DeFi ~~products, services,~~ arrangements~~, and activities~~ that are subject to Existing Frameworks and New Frameworks, including measures to detect, deter, enforce, sanction, redress and correct violations of applicable laws and regulations. A regulator should assess what technological knowledge, skills, resources, data and tools the regulator needs to appropriately enforce applicable laws.

Recommendation 8 (Promote Cross-Border Cooperation and Information Sharing): A regulator, in recognition of the cross-border nature of DeFi ~~products, services,~~ protocols and arrangements ~~, and activities,~~ should have the ability to cooperate and share information with regulators and relevant authorities in other jurisdictions with respect to identifying such protocols and arrangements~~, and activities~~ in order to facilitate investigations and encourage

the development of common standards, as well as the harmonization and mutual recognition of regulatory requirements across jurisdictions. This includes leveraging existing or 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. A regulator should also set a minimum standard for procedural safeguards with respect to data confidentiality and the protection of personal privacy, as well as consistency in information sharing arrangements and requests, with a further goal of achieving consistency with existing safeguards to the extent possible.

Recommendation 9 (Understand and Assess Interconnections Among the DeFi Market, the Broader Crypto-Asset Market, and Traditional Financial Markets): When analyzing DeFi ~~products, services,~~ arrangements ~~, and activities~~, a regulator should seek to understand, including through consultation with DeFi stakeholders, the interconnections among the financial services (including financial products) provided through DeFi arrangements ~~used to offer financial services~~, 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, how these interconnections might present opportunities for improvements to traditional financial markets 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 use of DeFi ~~products, services,~~ arrangements ~~, and activities~~, including by taking into account evolving technological tools and best practices.

ANNEX 3: Flowchart Proposing How CDA and DeFi Recommendations Should Apply