July 31, 2023

International Organization of Securities Commissions
Calle Oquendo 12
28006 Madrid
Spain

By email: cryptoassetsconsultation@iosco.org

Re: GFMA Public Comment on IOSCO's Consultation Report on Policy Recommendations for Crypto and Digital Asset Markets

The Global Financial Markets Association (**GFMA**)[1] welcomes the opportunity to comment on the International Organization of Securities Commission's (**IOSCO**) "Policy Recommendations for Crypto and Digital Asset Markets – Consultation Report" (CDA Recommendations).[2] We support IOSCO's goals of encouraging greater consistency with respect to digital asset regulatory frameworks and oversight across jurisdictions, and addressing concerns related to market integrity and investor protection in digital asset markets, through its promulgation of policy recommendations.[3] Trust remains a foundational element of effective and robust capital markets. Regulatory policy is a core component of trust, ensuring market participants operate within a set of common rules that appropriately protect all stakeholders and meet the regulatory outcomes of policymakers. Balanced regulatory policy involves weighing growth and innovation with safety and soundness, market integrity, consumer protection, and overall financial stability.

As we have noted with respect to other, similar consultation reports, a principles-based and technology-neutral approach to crypto-assets that also takes into account existing regulatory regimes is the most appropriate approach to addressing crypto-asset regulation.[4] This approach is the one most consistent with the principle of "same activities, same risks, same regulatory

[1] GFMA represents the common interests of the world's leading financial and capital market participants to provide a collective voice on matters that support global capital markets. It also advocates on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows to end users. GFMA efficiently connects savers and borrowers, thereby benefiting broader global economic growth. The Association for Financial Markets in Europe (**AFME**) located in London, Brussels, and Frankfurt; the Asia Securities Industry & Financial Markets Association (**ASIFMA**) in Hong Kong; and the Securities Industry and Financial Markets Association (**SIFMA**) in New York and Washington are, respectively, the European, Asian, and North American members of GFMA.

[2] IOSCO, Policy Recommendations for Crypto and Digital Asset Markets – Consultation Report (May 2023), *available at* https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf.

[3] *Id.* at 1.

[4] *See, e.g.*, GFMA's Response to the Financial Stability Board's (**FSB**) International Regulation of Crypto-Asset Activities – A Proposed Framework (Dec. 15, 2022), *available at* https://www.gfma.org/wp-content/uploads/2022/12/gfma-response-to-fsb-crypto-asset-consult-15-december-2022.pdf (**GFMA FSB Response**); AFME's Response to HM Treasury Future Financial Services Regulatory Regime for Cryptoassets: Consultation and Call for Evidence (Apr. 28, 2023), *available at* https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_HMT%20Crypto%20Consultation%20Response%2028.04.23.pdf, Joint Trades' Response to BCBS 2nd Consultation on the Prudential Treatment of Cryptoasset Exposures (September 2022), *available at* https://www.gfma.org/wp-content/uploads/2022/10/joint-trades-comment-letter-second-consultation-on-prudential-treatment-of-cryptoasset-exposures.pdf.

outcomes," which both IOSCO[5] and we[6] support. Regulatory policy should seek to instill the same stability and protections in crypto-asset markets that exist in traditional, regulated financial markets while allowing and supporting innovation. Distributed ledger or blockchain technology (**DLT**) holds promise for unlocking efficiencies, driving growth, and harnessing such innovation. Payments, settlement, and lifecycle events may be accomplished with greater safety and more efficiency; access may be expanded to a broader set of participants; and such technology can support interoperability of markets and market infrastructure that may operate more effectively with improved liquidity. At scale, these developments could benefit the real economy. Where regulatory oversight and institutional risk management exists, this potential should not be ignored or prohibited.

In order to achieve these goals, it is critical that IOSCO as a global standard setter[7] does not treat all assets and institutions that make use of DLT alike. It is also important to distinguish among different types of DLTs, as we have detailed in a recent whitepaper "*The Impact of Distributed Ledger Technology in Global Capital Markets (May 2023)*" (the **GFMA Whitepaper**).[8] Analysis in the GFMA Whitepaper identified that market participants make decisions around technology across a range of use case-specific considerations.

As an initial matter, we note that DLT can be used as simply a technology for a firm's internal books and records, which does not present the same considerations as tokenization of assets using DLT and should not result in assets simply recorded by a firm internally using DLT being treated as "crypto-assets".[9] Then, where DLT is used to create a tokenized asset, there are different types of DLT. "Private-permissioned" networks present limited incremental considerations that can be addressed by leveraging existing regulatory processes and therefore are analogous to technology operating in capital markets today. They introduce efficiencies and a platform for innovation, such as programmable security products. Where the legal nature of a service or a function does not change, the use of DLT-based systems to support or record the provision of that service or function should not result in incremental risk or necessitate a change in the regulation or regulatory characterization of that service or function. Policymaking should allow such networks to exist and flourish if demand warrants. Public networks ("public-permissioned," "public-permissionless") have their own set of network-specific considerations that should be evaluated in the context of applicable use cases. Capital market participants have developed applications on private-permissioned, public-permissioned, and public-permissionless networks, choosing the specific configuration best suited for their business needs to serve clients efficiently within their own risk

[5] CDA Recommendations at 1.

[6] *See* sources cited *supra* note 4.

[7] "The International Organization of Securities Commissions (**IOSCO**) is the international body that brings together the world's securities regulators and is recognized as the global standard setter for securities regulation. IOSCO develops, implements, and promotes adherence to internationally recognized standards for securities regulation. It works intensively with the G20 and the FSB on the global regulatory reform agenda." (*IOSCO Processes for Policy Development and Implementation Monitoring*).

[8] *See* GFMA, et al., Impact of Distributed Ledger Technology in Global Capital Markets (May 17, 2023), *available at* https://www.gfma.org/wp-content/uploads/2023/05/impact-of-dlt-on-global-capital-markets-full-report.pdf at 2.

[9] *See* GFMA Whitepaper at 15-17.

management frameworks. Key to the success of DLT-based solutions is support by policymakers for responsible innovation and flexible best practices for institutions to set controls based on the size, scope, and complexity of a given use case.

In light of these circumstances, rather than taking a categorical approach, such as prohibiting firms from using a particular type of technology, regulators should ensure that firms develop, test, and apply existing and emerging risk mitigation best practices and technologies to manage and mitigate risk.[10] Use of such best practices and technologies to fulfill regulatory requirements related to, for example, trade and counterparty identification and surveillance, as well as know-your-customer (**KYC**) compliance, will help to address core investor and customer protection and market integrity mandates without stymieing the development and use of new technologies.

We appreciate the crypto market context in which the CDA Recommendations were developed, including the shock events that took place during 2022 and 2023. Given the opportunities and the risk management nuances of DLT as summarized above, we respectfully submit that these particular market events, which arose in connection with unregulated or lightly regulated institutions, do not flow inherently from use of DLT, or the asset classes that leverage the technology, but rather were driven primarily by weaknesses in the corporate governance structures and risk management principles of the particular service providers at issue.

Indeed, those events would have been much less likely to have occurred—and customers much less likely to have faced such dramatic losses—had the relevant entities been subject to established supervisory policies and procedures by both market and prudential regulatory authorities. In this regard, consistent with the principle of "same activities, same risks, same regulatory outcomes," all firms—whether an established, traditional financial institution or a crypto-asset-native startup—that engage in the same type of activity in the crypto-asset markets should be subject to the same regulatory regime.

Over the last few years, there have also been many important applications of DLT within traditional, regulated market settings, in which the technology can provide significant risk mitigation and efficiency benefits.[11] In these instances, the use of DLT itself should not drive different regulatory outcomes. Such a technology-driven, as opposed to technology-neutral, approach would have the effect of creating regulatory conflicts and burdens where DLT-driven regulations overlap with traditional ones, or where different rules apply but do not overlap, fostering regulatory arbitrage and market fragmentation, and stifling innovation. None of these outcomes is consistent with IOSCO's objectives.

[10] *See* IOSCO Principles for Financial Market Infrastructure (April 2012); Principles on Outsourcing (Oct. 2021); Operational Resilience of Trading Venues and Market Intermediaries During the Covid-19 Pandemic (Jan. 2022); BCBS Principles for Operational Resilience and Principles for Sound Management of Operational Risk (March 2021); FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting and Format for Incident Reporting Exchange (FIRE) (April 2023); and the FSB Consult on Critical Third Parties (June 2023).

[11] *See* GFMA Whitepaper.

In light of these considerations, it is critical that IOSCO members follow a process of: first, identifying whether (or which) existing regulations apply to a particular asset, service or institution within the lifecycle of the trade;[12] second, filling any regulatory gaps (if any) that exist for making use of technology (*e.g.*, DLT); and third, if existing regulations apply but do not account for particular risk characteristics of the technology or the asset, making targeted modifications to those regulations.

In this regard, below we lay out six foundational pillars that IOSCO leadership and members should aim to address when finalizing its CDA Recommendations:

> **Pillar I:** IOSCO Should Provide Classification Approach Delineating the Types of Digital Assets Covered by Each of the Recommendations to Avoid Conflicts and Overlaps with Regulation of Traditional Financial Markets
>
> **Pillar II:** IOSCO Should Clarify the Scope of CASPs Covered by the Recommendations to Avoid Conflicts and Overlaps with Regulation of Traditional Financial Institutions
>
> **Pillar III:** IOSCO Should Tailor the Application of Its Recommendations to Account for the Capacity in Which a CASP Is Acting
>
> **Pillar IV:** IOSCO Should Tailor the Application of Its Recommendations Depending on Type of Client or Counterparty
>
> **Pillar V:** IOSCO Should Modify Its Recommendations to Account for Varying Market Structures
>
> **Pillar VI:** IOSCO Should Recognize the Need to Accomplish Settlement Finality and Legal Certainty Within the Different Circumstances of Applicable Network Structure

In addition, we have laid out in Annex A responses to the proposed CDA Recommendations which reflect these steps for developing new policy. Annex A also includes our proposed revisions (in *red text*) to the text of the specific Recommendations (in *blue text*) to provide constructive feedback to help achieve IOSCO's objectives. These suggestions build off of those provided in the GFMA Whitepaper, and we encourage IOSCO to consult that document in its entirety as it finalizes its recommendations.[13]

[12] Today this is a complex and challenging task for both market participants and regulators, particularly given that crypto-assets are not currently categorized in a consistent way across jurisdictions. We encourage IOSCO to review the GFMA Whitepaper and the associated taxonomy, *see infra* note 28, which proposes a path forward with respect to crypto-asset classification.

[13] In particular, Chapter 4 of the GFMA Whitepaper discusses the current legal and regulatory landscape, and proposed considerations for next steps, and Recommendation #1 addresses actions to promote legal certainty and regulatory clarity.

Pillar I: IOSCO Should Provide Classification Approach Delineating the Types of Digital Assets Covered by Each of the Recommendations to Avoid Conflicts and Overlaps with Regulation of Traditional Financial Markets

The CDA Recommendations define the term "crypto-asset," to refer to an asset that is issued and/or transferred using DLT, including, but not limited to, so-called "virtual currencies," "coins," and "tokens."[14] This definition focuses on the use of DLT, not the economic or legal characteristics of the asset. The relevant market events identified by the CDA Recommendations, however, were not driven inherently by the use of DLT, nor do they appropriately exemplify all uses of DLT in recent years. As noted above, DLT is seeing increasing use in traditional, regulated financial markets as well, involving the tokenization of real-world assets and underlying securities, driven by investor and client demand for enhanced efficiencies that can be derived from this technology.

Unintended consequences for market structure and services currently offered by regulated entities could result from treating applications of DLT in traditional asset classes in the same manner as cryptocurrencies and other, more recently developed digital asset types. IOSCO's broad definitional approach of crypto-assets could lead to regulatory conflicts and would be inconsistent with how other global standard setters are approaching the topic (*i.e.*, by providing differentiated classifications based on specified criteria and risk factors).[15] For example, DLT has been used to tokenize commercial bank deposits. Although tokenized commercial bank money shares the "stable value" characteristic with stablecoins, applying the CDA Recommendations' stablecoin-related recommendations in this context would fail to account for the well-developed economic and regulatory framework for deposit-taking institutions.[16] Similarly, treating deposit liabilities like custodial liabilities with related segregation and other restrictions on use of client funds would (1) limit the provision of custody services by traditional financial intermediaries, (2) stymie bank lending activity and run counter to the established role that bank intermediation plays in the funding and credit markets and (3) limit access for established financial service providers such as custody banks to offer their services in these nascent markets and provide required stability and consumer protection.[17]

Another unintended consequence example relates to tokenized stocks, bonds and other traditional securities. The existing regulatory regime for traditional, non-DLT securities (*i.e.*, with respect to custody, trading, clearing and settlement) already applies to these tokenized securities; a new, comprehensive regulatory regime addressing these topics is not needed and could lead to onerous

[14] CDA Recommendations at 3, n.5.

[15] For example, other international regulatory bodies have recognized distinctions among tokenized traditional assets, stablecoins and other types of cryptoassets. *See, e.g.*, Basel Committee on Banking Supervision, Prudential treatment of cryptoasset exposures (Dec. 2022), *available at* https://www.bis.org/bcbs/publ/d545.pdf (classifying Group 1 and Group 2 cryptoassets and setting different capital standards for each).

[16] *See also* Annex A, Responses to Chapter 10.

[17] *See also* Annex A, Responses to Chapter 7.

and conflicting requirements that could ultimately hinder the functioning and regulation of digital assets and markets.

Specifically, Recommendation 4 would require "a [crypto-asset service provider (**CASP**)], when acting as an agent, to handle all client orders fairly and equitably . . . [and] to have systems, policies and procedures to provide for fair and expeditious execution of client orders."[18] But existing regulated securities firms, which could fall within the CDA Recommendations' broad definition of a CASP, are already subject to order handling requirements (including best execution) when they act as agents in handling client orders for securities. The CDA Recommendations' proposed standard for handling client orders would depart from preexisting best execution requirements for these firms, which focus on obtaining the favorable results for the client taking into account relevant market conditions and other factors, rather than on "fair" or "expeditious" execution.[19] We are concerned that an "expeditious" execution requirement could be (mis)interpreted to require fast or immediate execution, when best execution under existing regulations could require something else (*e.g.*, for larger orders).[20] Ultimately, this recommendation could result in unhelpful and conflicting guidance that is onerous and potentially impractical for CASPs to operationalize.[21]

In these instances where existing regulations already apply, IOSCO should only recommend incremental revisions to account for (1) differentiated risks that may arise due to the use of new technologies like DLT (*e.g.*, security of digital asset private keys)[22] and (2) the fact that certain existing rules may not be applicable (or applicable in the same way) to digital ledger technology (*e.g.*, when transacting using a blockchain, there may not be a central clearing counterparty (**CCP**) intermediating between buyers and sellers, and so existing CCP regulations may not be relevant).[23]

Distinguishing among different types of digital assets along these lines will help to ensure that the recommendations are applied in a thoughtful, appropriate and nuanced way in order to avoid regulatory gaps and arbitrage possibilities, and ensure the regulations are fit for purpose. For

[18] CDA Recommendations at 19.

[19] For example, Financial Industry Regulatory Authority (**FINRA**) Rule 5310 requires U.S. broker-dealers to use "reasonable diligence to ascertain the best market for the subject security and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions." Rule 5310 also provides a list of illustrative factors that it will consider in determining whether a member has used "reasonable diligence"—fairness and expeditiousness are not included.

[20] It is also not clear how a CASP could demonstrate that execution was "fair."

[21] Other jurisdictions also have existing regulatory regimes which could conflict with this and other recommendations. *See, e.g.*, GFMA Whitepaper (discussing, among other things, the Markets in Financial Instruments Directive (**MiFID II**) and Central Securities Depositories Regulation (**CSDR**) regimes in Europe). *See also* Annex A, Responses to Chapter 3.

[22] Use of DLT with respect to a traditional asset does not necessarily increase or fundamentally transform the risk of that asset. In fact, in many instances, DLT would reduce risk. *See, e.g.*, Joint Trades including GFMA, Comments in Response to the 2nd Consultative Document on the Prudential Treatment of Cryptoasset Exposures (September 2022), (noting that, among other things, DLT "would help mitigate counterparty, liquidity and settlement risk" (thereby improving risk management tools)).

[23] *See also* Annex A, Response to Question 2.

example, Recommendation 6 would require a CASP to establish, maintain, and disclose standards for listing (or removing from listing) digital assets for trading.[24] We agree with this recommendation, generally, but it should acknowledge that appropriate listing standards are likely to differ based on the type of digital asset. Traditional financial market regulations take these differences into account. In the United States, for example, listing standards for equity securities focus on, among other things, adequacy of disclosure, based on the general principle that potential investors in a public company should have access information about the firm before investing,[25] while listing standards for commodity derivatives focus on, among other things, whether the instrument is readily susceptible to manipulation, given that the value of the derivative depends upon the characteristics of the underlying commodity.[26]

To help facilitate such distinctions, we would draw IOSCO members' attention to our recently published GFMA Whitepaper,[27] in which we proposed an approach to the classification of digital assets, and which we respectfully request IOSCO consider in connection with any final policy recommendations.[28] Among other things, the taxonomy in the GFMA Whitepaper proposes six types of digital assets based on their differing characteristics (*see* Annex B). As we noted in the GFMA Whitepaper, distinguishing among digital assets "reflects the principle that the treatment of digital-assets should be underpinned by clear methodology … [and] allow for tailored regulatory treatment."[29] Such methodology should also be flexible to account for evolving nature of crypto-assets and the associated technology.

Pillar II: IOSCO Should Clarify the Scope of CASPs Covered by the Recommendations to Avoid Conflicts and Overlaps with Regulation of Traditional Financial Institutions

The CDA Recommendations define the term "CASP" to refer to "service providers that conduct a wide range of activities relating to crypto-assets, including but not limited to, admission to trading, trading (as agent or principal), operating a market, custody, and other ancillary activities such as lending/staking of crypto-assets and the promotion and distribution of crypto-assets on behalf of others."[30] The proposed CASP definition provides a non-exhaustive list of activities relating to

[24] CDA Recommendations at 22. The application of this recommendation to all CASPs, without distinguishing between the role that CASP plays in the market, is also problematic. This letter provides a detailed discussion of this concern.

[25] *See, e.g.*, Form S-1, *available at* https://www.sec.gov/files/forms-1.pdf (requiring detailed disclosure of the registrant).

[26] *See, e.g.*, 17 C.F.R. § 38.200-201. *See also* Annex A, Responses to Chapter 4.

[27] GFMA Whitepaper, *supra* note 8.

[28] *Id.* at Annex 1, *available at* https://www.gfma.org/wp-content/uploads/2023/05/annex-1-gfma-proposed-approach-for-the-classification-and-understanding-of-digital-assets.pdf (**GFMA Taxonomy**). We note that authorities have likewise recognized risk-based distinctions among different types of crypto-assets in other contexts. *See, e.g.*, Basel Committee on Banking Supervision, Prudential treatment of cryptoasset exposures (Dec. 2022), *available at* https://www.bis.org/bcbs/publ/d545.pdf.

[29] *Id.* at 181.

[30] CDA Recommendations at 1, n.4. Other international standard setting bodies have also proposed definitions in relation to crypto-assets and firms engaged in crypto-asset activities. *See, e.g.*, Financial Action Task Force (**FATF**), *Virtual Assets and Virtual Asset Service Providers* (Oct. 2021), *available at* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (defining "virtual asset" and

crypto-assets that would result in a service provider being a CASP, but it notably does not include other types of activities, such as being a crypto-asset issuer. In this regard, the CASP definition could be overbroad or too narrow, based on the relevant circumstances. For this reason, it is important for the CDA Recommendations to take a more nuanced approach rather than applying all Recommendations to all CASPs (as defined) in the same way.

In addition to defining the term CASP to encompass a variety of different functions, the CDA Recommendations do not treat CASPs differently depending on whether they are otherwise comprehensively regulated. In many instances, however, those regulations, even when not specific to crypto-assets, already address areas covered by the CDA Recommendations. These areas include conflicts-of-interest mitigation, management of material non-public information (**MNPI**), custody of client assets, capital requirements, and management of operational and technology risks.

Regulated banks, brokers, and dealers already face comprehensive regulation in these and other areas, which would conflict or overlap with the CDA Recommendations. For example, the CDA Recommendations propose a number of recommendations with respect to custodial services[31] and would apply those recommendations to all CASPs, without distinguishing among different types of CASPs.[32] But certain CASPs are already subject to appropriate regulation with respect to their custody services and additional requirements may not be needed. A CASP that, for example, is a Securities and Exchange Commission (**SEC**) registered broker-dealer must already comply with strict rules regarding, among other things, customer asset protection and capital and financial resources requirements—an entirely new regulatory regime for tokenized securities is not needed merely due to the introduction of a new technology.[33]

To clarify for members of IOSCO, the starting point for the recommendations, therefore, should be whether existing regulations are sufficient. Only after determining that there is some gap should an IOSCO member consider recommending additional requirements. For firms that are already subject to regulation, it may well be that no changes, or only incremental ones, are necessary. In this regard, we note that traditional financial institutions regularly make use of new technologies

"virtual asset service provider" (**VASP**)). Although they may overlap in part, our understanding is the definitions are distinct and not to be used interchangeably because they are intended to address different objectives.

[31] *Id.* at 31-37 (Recommendations 13-16).

[32] For example, Recommendation 13 would "require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets." *Id.* at 32. Since certain CASPs may not custody client assets at all (or may, for example, provide other, related services, such as a reporting service on "not-in-bank" assets), this is a good example of where the CDA Recommendations could take a more granular approach to the application of the recommendations to particular types of CASPs.

[33] *See, e.g.,* 17 C.F.R. § 15c3-3 (SEC rule requiring broker-dealers to, among other things, maintain custody of customer securities and safeguard customer cash by segregating these assets from the firm's proprietary assets); 17 C.F.R. § 15c3-1 (SEC rule setting capital requirements); Regulation Q, 12 C.F.R. § 217 (Board of Governors of the Federal Reserve System (**Federal Reserve**) rule setting capital requirements). These examples are not meant to suggest that all CASPs should be subject to the SEC's or the Federal Reserve's regime—many other jurisdictions also have their own custody regulations that already apply to traditional financial market custodians (and could apply to CASPs in those jurisdictions).

and apply their existing risk management tools and supervisory safeguards to them without new regulatory mandates—the use and management of DLT is no different.

For unregulated firms, we would expect that recommendations would, as an initial matter, require those firms to comply with the same applicable regulatory and licensing regimes as are applicable to currently regulated firms conducting the same activities, though more comprehensive recommendations may be appropriate if the existing regimes are not fully applicable or result in gaps based upon a particular firm's activities. An entity that, for example, operates a market or acts as custodian or market maker for assets using DLT should be subject to the same core regulatory and licensing framework as an entity that provides those services for non-DLT assets.[34] And an entity that is already regulated need not be subject to an entirely new regulatory regime or licensing requirement merely because it starts to use a new technology such as DLT; instead, only incremental changes required to account for differentiated risks posed by the technology need to be implemented. In making such incremental changes, regulators should account for the fact that technological solutions are likely to continue to evolve, and regulatory guidance should therefore be flexible, not prescriptive.

In sum, for clarity for IOSCO members globally as they develop policy approaches, it would more generally be appropriate to use the term CASP solely to refer to the unregulated firms, with regulated firms instead only subject to any of the CDA Recommendations in instances where their crypto-asset activities are not already subject to regulation in the area covered by a particular recommendation (*e.g.*, if a securities broker-dealer is providing services in crypto-assets that are not securities and thus not subject to relevant securities regulations for those services, it should be regulated in accordance with the CDA Recommendations for those non-securities crypto-assets). Traditional market participants, both in the private and public sectors, benefit from legal precedent and cross-border legal certainty. The introduction of the term CASP with broad application could reintroduce risks of market fragmentation and conflicts of law for established markets.

Pillar III: IOSCO Should Tailor the Application of its Recommendations to Account for the Capacity in Which a CASP Is Acting

With perhaps one exception (Recommendation 4, concerning order handling), the CDA Recommendations do not clearly distinguish among the different capacities in which CASP may act and whether the recommendation applies to all capacities in which a CASP is acting. Under current laws in traditional markets, firms that operate trading facilities are subject to different requirements when acting in that capacity than when they act as brokers or dealers or custodians or lenders. And even among those operating trading facilities, existing regulations distinguish between those who perform self-regulatory responsibilities and those who do not. We recognize that, in certain crypto-asset markets, some participants commingle these functions. But given the CDA Recommendations to address such commingling, we think it is necessary to take into account

[34] *See also* Annex A, Response to Question 2.

the particular capacity in which a CASP is acting such that its recommendations are tailored to the roles that different CASPs play in the digital asset markets.

Take, for example, the CDA Recommendations to address abusive behaviors.[35] Recommendation 9 provides that there should be market surveillance requirements that apply to each CASP in order to mitigate market abuse risks.[36] While we, of course, support market surveillance regulations, the recommendations should acknowledge these requirements must differ based on a CASP's particular role. The regulatory regime applicable to the derivatives markets in the United States is illustrative. Derivatives exchanges, such as designated contract markets (**DCMs**), are required by Commodity Futures Trading Commission (**CFTC**) regulations to prevent market manipulation and price distortions by setting and enforcing rules for trading on their platforms.[37] The CFTC monitors DCMs to ensure that such rules are in place and appropriately enforced.[38] On the other hand, futures commission merchants (**FCMs**) and other firms that transact on DCMs must comply with the DCM's rules, as well as the CFTC's rules prohibiting manipulation.[39] While DCMs, FCMs and trading entities are all subject to rules regarding market abuse, those rules differ based on the role that each such entity plays in the market. The same holds true for CASPs—a CASP that operates a digital asset exchange should be subject to different requirements than a CASP that trades on that exchange. The recommendations should take these differences into account.[40]

Pillar IV: IOSCO Should Tailor the Application of its Recommendations Depending on Type of Client or Counterparty

In one instance (Recommendation 18, concerning retail distributions), the CDA Recommendations distinguish between when a CASP is providing services to retail clients versus a professional or institutional counterparty. In traditional markets, however, this distinction can apply in a broader range of contexts, including in areas relating to order handling and client asset protection. And while it is the case that crypto-asset markets include significant retail components, DLT may also be used more broadly in institutional contexts as well. Accordingly, with respect to recommendations that involve interactions with clients or customers (*e.g.*, those addressing disclosure, order handling, etc.), the CDA Recommendations should more generally take into account whether the CASP is transacting with, or providing services to, retail or

[35] CDA Recommendations at 25-28.

[36] *Id.* at 26.

[37] *See* 17 C.F.R. § 38.150-160, 250-258. DCMs themselves are not trading firms that transact on the DCM's trading platform.

[38] *See, e.g.*, Rule Enforcement Reviews of Designated Contract Markets, *available at* https://www.cftc.gov/IndustryOversight/TradingOrganizations/DCMs/dcmruleenf.html.

[39] 17 C.F.R. § 180.

[40] *See also* Annex A, Response to Recommendation 9. As an example, we would note that Title Vi, Chapter 3 of the EU's Markets in Crypto-Assets Regulation (**MiCA**) has explicitly differentiated requirements for different types of CASPs, including operation of a crypto-asset trading platform, custody and administration of crypto-assets, , placing and execution of crypto-asset orders and crypto-asset advisory services.

professional/institutional counterparties and refine the recommendations where appropriate to account for this distinction.[41]

Pillar V: IOSCO Should Modify Its Recommendations to Account for Varying Market Structures

In traditional financial markets, regulation varies, sometimes significantly, depending on the applicable market structure. For example, the U.S. regulatory regime is quite different for equity securities that may trade on a national securities exchange (**NSE**)[42] than for bonds that trade on an alternative trading system (**ATS**)[43] or the securities of a private issuer that trade OTC.[44] Because of different market structure, the regulation of commodity derivatives markets also varies significantly, not just from the securities regulatory regime but also based on the type of derivative.[45] The CDA Recommendations should, likewise, consider market structure in setting final recommendations for digital asset markets and CASPs. This consideration is especially relevant in connection with order handling and trade disclosures, where differences in linkages among trading venues and calibration of public dissemination rules can have enormous negative consequences for market efficiency and integrity.[46]

Pillar VI: IOSCO Should Recognize the Need to Accomplish Settlement Finality and Legal Certainty Within the Different Circumstances of Applicable Network Structure

In addition to the structural and behavioral issues noted in the CDA Recommendations, a further key building block for market integrity lies in the ability to achieve requisite legal certainty to ensure that settlement of transactions is final.[47] The GFMA Whitepaper addresses this issue,

[41] *See also* Annex A, Responses to Questions 5, 10, 16 and 18. It may be the case that certain CASPs transact with or provide services to both retail and professional/institutional customers. For example, certain CASPs operate markets that are accessible by all types of customers (and others might operate markets that limit access to a particular type of customer). The same holds true in traditional financial markets due to certain regulatory requirements and market structure evolution. The recommendations should, therefore, also take into account the possibility that CASPs may offer services to all types, or only certain types, of customers.

[42] *E.g.*, Regulation NMS 17 C.F.R. § 242.600-614. *See also* SEC, Proposed Order Competition Rule (Dec. 14, 2022), *available at* https://www.sec.gov/rules/proposed/2022/34-96495.pdf.

[43] *E.g.*, Regulation ATS, 17 C.F.R. § 242.300-304.

[44] For example, as noted above, a national securities exchange cannot accept for listing the equity securities of a company unless that company publicly discloses a substantial amount of information. And such companies are subject to ongoing disclosure requirements. *See, e.g.,* Form 10-K. A broker-dealer seeking to publish quotations in OTC securities, on the other hand, is subject to entirely different (and, in certain regards, less burdensome) information disclosure requirements. *See* 17 C.F.R. § 15c2-11. Recommendation 6, which would require a CASP to establish, maintain and disclose crypto-asset listing standards, should acknowledge that varied market structure could mean that listing standards for different digital assets and CASPs should also vary.

[45] For example, different rules and conventions have evolved to govern exchange-traded futures, *e.g.*, 17 C.F.R. § 38, swaps traded on a swap execution facility, *e.g.*, 17 C.F.R. § 37, and swaps traded OTC, *e.g.*, the ISDA Master Agreement and ancillary documentation.

[46] *See also* Annex A, Responses to Chapter 3.

[47] *See also* Annex A, Response to Question 15(c).

noting the relevant risks and mitigants for different network archetypes.[48] Given the importance of this topic, and the fact that best practices with respect to settlement finality in the context of on-chain DLT transfer may differ from those in traditional markets and also continue to evolve, we encourage regulators to engage with market participants in particular in this area. In this regard, the GFMA encourages IOSCO to foster regulatory and legislative programs that provide parties with appropriate incentives to continue to develop technological solutions that support legal certainty and settlement finality.

* * *

The development of the digital asset ecosystem motivates all market stakeholders to look to the future. We value the coordination the IOSCO Fintech Task Force has taken with other global standard setters (*e.g.*, BCBS) and financial stability coordinating bodies (*e.g.*, FSB). Similar to the BCBS adopting a classification approach to evaluating risk of digital assets, we urge IOSCO as another global standard setter to also adopt the principle that the treatment of crypto-assets should be underpinned by clear methodology for identifying different types of digital assets to allow for tailored regulatory treatment, as appropriate, to mitigate reputational risks that could arise by conflating all use cases of DLT as "crypto," promoting legal clarity and confidence for asset managers, investors and issuers.

We very much appreciate the opportunity to comment on the CDA Recommendations and we look forward to engaging with IOSCO further, as may be helpful. If you have any questions, or you would like to discuss the points raised in this letter, please feel free to contact us as we look forward to ongoing collaboration on this important topic.

Yours faithfully,

Allison Parent

Allison Parent
Executive Director
Global Financial Markets Association (GFMA)
aparent@global.gfma.org
www.gfma.org

[48] *See, e.g.*, GFMA Whitepaper at 26.

Annex A

This Annex sets out our responses to the CDA Recommendations' questions for consultation. It also includes our proposed revisions (in *red text*) to the proposed text of the Recommendations (in *blue text*).

Chapter 1: Overarching Recommendation Addressed to All Regulators

Question 1: Are there other activities and/or services in the crypto-asset markets which Recommendation 1 should cover? If so, please explain.

Recommendation 1 should also cover staking and yield farming to the extent facilitated by intermediaries. Staking generally refers to the process by which the holder of a token native to a proof-of-stake blockchain commits (that is, "stakes") that token to a validator node on that blockchain in order to facilitate the validation of transactions via network consensus on the blockchain in return for compensation (sometimes called "rewards"), typically in the form of additional native tokens.[49] Yield farming generally refers to the process by which a crypto-asset holder deploys their crypto-assets in a manner intended to maximize returns (or "yield"), which may be done using various crypto-asset and decentralized finance (**DeFi**) protocols and applications, such as lending protocols or automated market maker protocols. When participation in these processes is facilitated by intermediaries, it may be appropriate to adopt safeguards around the role of the intermediary, such as disclosure with respect to the terms, conditions, risks and any conflicts of interest associated with the intermediary's role, as well as interaction with custody/safekeeping rules.[50]

Question 2: Do respondents agree that regulators should take an outcomes-focused approach (which may include economic outcomes and structures) when they consider applying existing regulatory frameworks to, or adopting new frameworks for, crypto-asset markets?

We endorse Recommendation 1 and support an outcomes-focused, principles-based and technology-neutral approach to the regulation of crypto-asset markets. In seeking to achieve the same regulatory outcomes, regulators should, to the greatest extent possible, apply the same rulesets to entities that are engaged in the same type of activities, as opposed to seeking to achieve

[49] We note that such regulation should be designed not to hinder the ability to participate in the underlying staking processes or lending/trading protocols or applications. In particular, broad participation in staking to generate network consensus in the validation of transactions is essential to promoting network security and stability.

[50] We recognize that the CDA Recommendations "do not cover [DeFi] activities, products or services" and that a separate consultation report will be published later this summer. CDA Recommendations at 1. We look forward to responding to that consultation and expect to provide comments regarding the appropriate scope of the definition of DeFi and regulation of crypto-asset trading activities that do not involve CASPs or other intermediaries.

the same objectives through different rulesets, which is likely to lead to regulatory arbitrage and other unintended consequences.[51]

An example of the implementation of this approach, which should be included in the explanatory text accompanying Recommendation 1, is as follows: "Regulators should ensure a consistent approach to regulatory licensing by, for example, requiring that a firm that provides custodial services in crypto-asset markets must be licensed as a custodian. However, an entity that is already licensed (*i.e.*, because it provides custody services to traditional financial assets) need not be subjected to an additional licensing requirement merely because certain assets custodied by the entity use DLT."

We have also included below some suggested changes to the text of the Recommendation 1.

Recommendation 1 (Common Standards of Regulatory Outcomes): Regulators should use existing frameworks or New Frameworks to regulate and oversee crypto-asset trading, other crypto-asset services, and the issuing, marketing and selling of crypto-assets (including as investments), in a manner consistent with IOSCO Objectives and Principles for Securities Regulation and relevant supporting IOSCO standards, Recommendations, and good practices (hereafter "IOSCO Standards"). The regulatory approach should seek 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 distributed ledger technology is used (i) in connection with traditional financial instruments or (ii) by traditional financial market service providers, regulators 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.

Chapter 2: Recommendations on Governance and Disclosure of Conflicts

Question 3: Does Chapter 2 adequately identify the potential conflicts of interest that may arise through a CASP's activities? What are other potential conflicts of interest which should be covered?

Chapter 2 should also consider the following potential conflicts of interests:

- A CASP may operate a validator node on a particular proof-of-stake blockchain, and also execute transactions on the blockchain; and
- A CASP that operates a market that is a self-regulatory organization (**SRO**) or a financial market infrastructure (**FMI**) may also be a trading participant on that platform, even as it has supervisory authority over competing trading participants.

[51] We note that this is the approach taken by the European Union in its Regulation on Markets in Crypto Assets (**MiCA**). In particular, MiCA Recital 9 provides that "Union legislative acts on financial services should be guided by the principles of 'same activities, same risks, **same rules**' and of technology neutrality" (emphasis added).

The CDA Recommendations already generally highlight the potential conflicts of interest concerns that may arise from vertically integrated crypto-asset trading platform business models. We agree with the CDA Recommendations' focus on potential conflicts of interest in those circumstances.[52]

The CDA Recommendations should also consider potential conflicts between a CASP and its non-CASP activities or non-CASP affiliates. For example, a CASP may have an affiliated or otherwise related venture capital firm that invests in (and has information and other rights with respect to) other crypto-asset projects that may compete with the CASP. As another example, a CASP may issue a token (other than a payment stablecoin) that is a debt or equity obligation of the CASP or which otherwise derives its value from the CASP, execute transactions in the native token, and also use that token in other ways (*e.g.*, for lending or collateral purposes). The CDA Recommendations touch on these situations in connection with Recommendation 7, which concerns management of primary market conflicts, but they should be addressed more holistically (*e.g.*, also requiring margin or collateral requirements to address wrong-way risk).

Additionally, as is the case in traditional financial markets, it would be helpful to consider conflicts of interests that could arise with respect to the employees or other people affiliated with a CASP. Certain employees may, for example, have access to MNPI. As described in response to Question 11 below, CASPs should have policies and procedures to mitigate conflicts of interest in these circumstances. As another example, CASPs should have policies and procedures to ensure that employee compensation practices do not incentivize undesirable behaviors, such as excessive risk-taking.

As described above, we also think it is important when considering potential conflicts of interest to distinguish among different types of CASPs, activities and customers when determining appropriate regulation in this regard.

***<u>Question 4</u>*: Do respondents agree that conflicts of interest should be addressed, whether through mitigation, separation of activities in separate entities, or prohibition of conflicts? If not, please explain. Are there other ways to address conflicts of interest of CASPs that are not identified?**

We support IOSCO's goal of ensuring appropriate mitigation of conflicts of interest. In particular, conflicts of interest involving CASPs should be addressed in the same manner as those of other, traditional financial services providers, with a focus principally on the use of information partitions and disclosures, as well as operational or legal entity segregation if a firm deems that approach necessary in order to mitigate conflicts of interest. Consistent with the approach taken in traditional financial markets, separation into different legal entities or unaffiliated parties should only be required in limited circumstances where such measures have been determined not to be sufficient, such as where a CASP also operates as an SRO. For example, in the United States, an

[52] CDA Recommendations at 5 ("Many CASPs typically engage in multiple functions and activities under 'one roof' – including exchange trading, brokerage, market-making and other proprietary trading, offering margin trading, custody, settlement, and re-use of assets – whether through a single legal entity or an affiliated group of entities that are part of a wider group structure.").

NSE (which is an SRO), cannot be affiliated with a broker-dealer (with the limited exception of operating a routing broker-dealer to fulfill Regulation NMS obligations). On the other hand, a broker-dealer operating an alternative trading system, which is not an SRO, may also make markets on that trading system and provide clearing, settlement, and custody services for subscribers to that platform, in each case subject to appropriate disclosure and information handling requirements.

***Question 5*: Does Recommendation 3 sufficiently address the manner in which conflicts should be disclosed? If not, please explain.**

CASPs should generally be permitted to make disclosures on a relationship-wide basis, including through websites and other readily accessible means, rather than, *e.g.*, requiring disclosure being made at the point of trade, which can impede trading and execution. In addition, disclosures should be tailored to the audience in question (*e.g.*, retail vs. professional/institutional) and not required to include "catchall" descriptions of immaterial conflicts or risks.

We have also included below some suggested changes to the text of the Recommendations 2 and 3.

Recommendation 2 (Organizational Governance): Regulators should require a CASP to have effective governance and organisational arrangements, commensurate to its activities, including systems, policies and procedures that would, amongst other things, address conflicts of interest, including those arising from different activities conducted, and services provided by a CASP or its affiliated entities. These conflicts should be effectively identified, managed and mitigated by the CASP and supervised by the regulator. Only in exceptional circumstances, such as where a CASP also exercises self-regulatory organization authority, should a ~~A~~ regulator ~~should~~ consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions.~~,~~ In these exceptional circumstances, a regulator ~~and~~ may require more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.

Recommendation 3 (Disclosure of Role, Capacity and Trading Conflicts): Regulators should require a CASP to have accurately disclosed each role and capacity in which it is acting (or may act) at all times. These disclosures should be tailored to the particular type of client and, for retail clients should typically be made, in plain, concise, non-technical language, as relevant to the CASP's retail clients, prospective retail clients, the general public, and regulators in all jurisdictions where the CASP operates, and into which it provides services. A CASP may consider whether more extensive disclosure using technical language is more appropriate for institutional or professional clients or prospective institutional or professional clients. Relevant disclosures should take place prior to entering into an agreement with a prospective client to provide services, and at any point thereafter when such position changes (e.g., if and when the CASP takes on a new, or different, role or capacity), though disclosures can be made on a relationship-wide basis, through websites and other readily accessible means, rather than on a transaction-by-transaction basis.

Chapter 3: Recommendations on Order Handling and Trade Disclosures

Question 6: What effect would Recommendations 4 and 5 have on CASPs operating as trading intermediaries? Are there other alternatives that would address the issue of assuring that market participants and clients are treated fairly?

We support requiring CASPs that handle customer orders as agent to do so in a manner that appropriately protects its customers. In this regard, please see our comments regarding order handling (including best execution) requirements provided in the letter above, in particular the inconsistency between the proposed "fair and expeditious" order handling standard and the standards that apply in traditional financial markets, as well as the need for order handling standards to account for relevant market structure for different types of assets.

Question 7: Do respondents believe that CASPs should be able to engage in both roles (i.e. as a market operator and trading intermediary) without limitation? If yes, please explain how the conflicts can be effectively mitigated

Subject to the conflict-of-interest comments set out above, a CASP should generally be permitted to engage in both roles, with appropriate safeguards of confidential client information (including information barriers), client disclosures and, as appropriate, operational and legal entity segregation (that is, not "without limitation").

Question 8: Given many crypto-asset transactions occur "off-chain" how would respondents propose that CASPs identify and disclose all pre- and post-trade "off-chain" transactions

In the first instance, whether pre- or post-trade disclosure obligations apply to a transaction should, consistent with the approach in traditional financial markets, depend on consideration of transparency and liquidity objectives, as well as relevant market characteristics. To the extent the characteristics of the relevant DLT in use for the transactions natively satisfy these requirements (*e.g.*, because transactions are broadcast (pre-trade) or recorded (post-trade) on a blockchain available to regulatory authorities and/or the public), then that use of DLT could, in such instance, potentially satisfy those requirements without use of other operational or technological mechanisms.

We have also included below some suggested changes to the text of the Recommendations 4 and 5.

Recommendation 4 (Client Order Handling): Regulators should require a CASP, when ~~acting~~ handling client orders as an agent and not as the operator of a market, to handle all client orders in a manner consistent with best execution standards applicable to client orders in traditional financial markets ~~fairly and equitably~~. Regulators should require a CASP to have systems, policies and procedures to provide for best ~~fair and expeditious~~ execution of client orders, and restrictions on front running client orders. Regulators should require that a CASP discloses these systems, policies and procedures to clients and prospective clients, as relevant. Orders should be ~~handled~~

~~promptly and~~ accurately recorded. A CASP that operates a market should handle orders submitted to the market neutrally and disclose its market's order matching and execution mechanics.

Recommendation 5 (Market Operation Requirements): Regulators should require a CASP that operates a market or acts as a market maker ~~an intermediary (directly or indirectly on behalf of a client)~~ to provide pre- and post-trade disclosures in a form and manner that are the same as, or that achieve similar regulatory outcomes consistent with, those that are required in traditional financial markets. Consistent with the approach taken in traditional financial markets, the extent and nature of such disclosures should take into account market liquidity and other relevant market structure characteristics.

Chapter 4: Recommendations in Relation to Listing of Crypto-Assets and Certain Primary Market Activities

Question 9: Will the proposed listing/delisting recommendations in Chapter 4 enable robust public disclosure about traded crypto-assets? Are there other mechanisms that respondents would suggest to assure sufficient public disclosure and avoid information asymmetry among market participants?

Please see our comments regarding listing and delisting standards provided in the letter above, as well as our comments regarding other potential conflicts of interest (*e.g.*, where a CASP that operates a market has an affiliated venture capital firm).

Question 10: Do respondents agree that there should be limitations, including prohibitions on CASPs listing and / or trading any crypto-assets in which they or their affiliates have a material interest? If not, please explain.

Instead of prohibiting a CASP from listing and/or trading in crypto-assets in which they or their affiliates have a material interest, any potential conflicts arising from such circumstances can be addressed through disclosures and other sales practice and governance regulations, similar to the approach taken in traditional financial markets.

For example, a structured products desk at a firm may create a product and that firm's asset management division may offer it to customers. The firm is not prohibited from creating and offering the product; instead disclosures, suitability standards, governance requirements and other safeguards apply (and may vary depending on whether the customer is retail or institutional).

It would not, in our view, be technology-neutral to apply a prohibition here merely because DLT is involved.

We have also included below some suggested changes to the text of the Recommendations 6 and 7.

Recommendation 6 (Admission to Trading): Regulators should require a CASP that operates a market to establish, maintain and appropriately disclose to the public their standards— including *systems, policies and procedures— for listing / admitting crypto assets to trading on its market, as well as those for removing crypto-assets from trading. These standards should take into account the nature and characteristics of the crypto-asset, and include the substantive and procedural standards for making such determinations. Regulators should endeavor to harmonize these standards to allow investors to compare listings across jurisdictions.*

Recommendation 7 (Management of Primary Markets Conflicts): Regulators should require a CASP to manage and mitigate conflicts of interest surrounding the issuance, trading and listing of crypto-assets. This should include appropriate disclosure, sales practice and governance requirements ~~and may necessitate a prohibition on a CASP listing and / or facilitating trading in, its own proprietary crypto-assets, or any crypto-assets in which the CASP, or an affiliated entity, may have a material interest~~. Regulators should also implement margin or collateral requirements, as appropriate, to address wrong-way risk if a CASP borrows or lends an asset it has issued.

Chapter 5: Recommendation to Address Abusive Behaviors

Question 11: In addition to the types of offences identified in Chapter 5, are there: (a) Other types of criminal or civil offences that should be specifically identified that are unique to crypto-asset markets, prevention of which would further limit market abuse behaviors and enhance integrity? or (b) Any novel offences, or behaviors, specific to crypto-assets that are not present in traditional financial markets? If so, please explain.

As noted above, one fact pattern that has arisen in the crypto-asset market context is that a CASP may operate a market, issue a token (other than a payment stablecoin) that is a debt or equity obligation of the CASP or otherwise derives its value from the CASP, execute transactions in that token in that market, and then also use that token for other purposes (*e.g.*, for lending or collateral purposes). In addition to requiring appropriate disclosure and conflict mitigation in order to reduce risk to customers, as well as margin or collateral requirements to address wrong-way risk, regulators should address the heightened potential for insider dealing or market manipulation that can arise with respect to these tokens. Regulators should also acknowledge that institutional customers should be expected to adhere to industry practices with respect to conducting appropriate due diligence with respect to the assets in which they trade.

Additionally, with respect to MNPI, CASPs, like traditional financial market providers, should use internal firewalls and information barriers, as appropriate, to mitigate the potential for insider trading-equivalent market abuse. Furthermore, CASPs should have policies and procedures that prohibit certain types of trading and other activities (at least with respect to employees with certain roles or access to certain information) and require all employees to complete internal compliance trainings, including with respect to conflicts of interest and MNPI.

There may be additional types of behaviors to consider in the DeFi context, though we expect to provide further comment on those in response to the forthcoming IOSCO DeFi consultation.

<u>Question 12</u>: Do the market surveillance requirements adequately address the identified market abuse risks? What additional measures may be needed to supplement Recommendation 9 to address any risks specific to crypto-asset market activities? Please consider both on- and off-chain transactions.

We strongly support requiring CASPs to have appropriate tools to identify, prevent and mitigate market abuse, including using tools to help identify parties to relevant transactions and transaction terms. Regulators should encourage firms to take into account evolving technological tools and best practices to address the core regulatory objectives of investor protection and market integrity, including where new technology may present greater opportunities for pseudonymity.[53] Regulators should not take a blanket approach either by prohibiting the use of certain technologies, which, as noted, could stifle industry growth and innovation, or applying one approach across different types of DLTs, since appropriate market surveillance tools will differ based on the characteristics of the relevant blockchain (*e.g.*, private versus public; permissioned versus permissionless). Within that context, regulators should consider in particular how the firms they regulate should address situations where other market participants engage in practices, such as "mixing," that present particular challenges to identifying relevant parties or transaction terms.

In this regard, permitting comprehensively regulated financial institutions to engage in crypto-asset market activities is likely to make such markets safer over time, given those institutions' well-developed compliance and surveillance tools, including with respect to anti-money laundering, counter-terrorism financing, and sanctions evasion. The converse is true as well—if regulated financial institutions are discouraged from engaging in these markets and using new technologies, then the crypto-asset markets are more likely to be used by those seeking to evade regulation and engage in harmful activities.

We have also included below some suggested changes to the text of the Recommendations 8, 9 and 10.

<u>Recommendation 8 (Fraud and Market Abuse)</u>: Regulators should bring enforcement actions against offences involving fraud and market abuse in crypto-asset markets, taking into consideration the extent to which they are not already covered by existing regulatory frameworks. These offences should cover all relevant fraudulent and abusive practices such as market manipulation, insider dealing and unlawful disclosure of inside information; money laundering / terrorist financing; issuing false and misleading statements; and misappropriation of funds and assets.

[53] *See, e.g.*, New York Department of Financial Services, Guidance on Use of Blockchain Analytics (Apr. 28, 2022), *available at* https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220428_guidance_use_blockchain_analytics (noting that "[p]otentially useful in [meeting KYC obligations] are products and services that allow their users to obtain identifying information (*e.g.*, location of a wallet address on a specific exchange for custodial transactions) that ties directly to the pseudonymous on-chain data, particularly in combination with customer-provided information.").

Recommendation 9 (Market Surveillance): Regulators should have market surveillance requirements applying to each CASP, taking into account the capacity in which the CASP is operating, so that market abuse risks are effectively mitigated.

Recommendation 10 (Management of MNPI): Regulators should require a CASP to put in place systems, policies and procedures, including internal firewalls and information barriers where appropriate, around the management of material non-public information, including, where relevant, information related to whether a crypto-asset will be admitted or listed for trading on its platform and information related to client orders, trade execution, and personally identifying information.

Chapter 6: Recommendation on Cross-Border Cooperation

Question 13: Which measures, or combination of measures, would be the most effective in supporting cross-border cooperation amongst authorities? What other measures should be considered that can strengthen cross-border co-operation?

We support multilateral coordination in order to (i) facilitate timely information-sharing around potentially abusive or otherwise inappropriate trading activity taking place across jurisdictions, (ii) encourage the development of best practices (for example, with respect to the development of standards for smart contracts program language to help promote interoperability and uniformity such that the technology reaches its full potential), and (iii) mitigate regulatory arbitrage across jurisdictions.

We have also included below some suggested changes to the text of the Recommendation 11.

Recommendation 11 (Enhanced Regulatory Cooperation): Regulators, in recognition of the cross-border nature of crypto-asset issuance, trading, and other activities, should have the ability to share information and cooperate with regulators and relevant authorities in other jurisdictions with respect to such activities in order to facilitate investigations, encourage the development of best practices and the harmonization of regulatory requirements across jurisdictions. This includes leveraging existing or having available cooperation arrangements and/or other mechanisms to engage with regulators and relevant authorities in other jurisdictions. These should accommodate the authorisation and on-going supervision of regulated CASPs, and enable broad assistance in enforcement investigations and related proceedings. Regulators should also set a minimum standard for procedural safeguards with respect to data confidentiality and the protection of personal privacy.

Chapter 7: Recommendations on Custody of Client Monies and Assets

Question 14: Do the Recommendations in Chapter 7 provide for adequate protection of customer crypto-assets held in custody by a CASP? If not, what other measures should be considered?

We generally support the proposal to adopt minimum standards around custody of client assets that are consistent with the standards and requirements that apply in traditional financial markets.[54]

Consistent with this approach of not applying different custody standards and requirements merely due to the use of DLT:

- Segregation of client assets from a CASP's proprietary assets should be recognized as an industry best practice and implemented.

- Segregation of one client's assets from another client's assets up the custody chain should, consistent with existing segregation requirements for traditional assets, be a commercial decision (rather than a regulatory requirement) that reflects the consideration of, among other things, cost and client asset protection. For example, requiring a retail client's crypto-assets to be segregated from the crypto-assets of all other retail clients could result in high costs to each such client due to a lack of economies of scale—for instance, in "gas" fees required to effect many individual transfers of small retail value.

- While we support appropriate segregation of client assets (and the existing regulatory regimes underpinning this concept), client cash held at a deposit-taking institution that is appropriately regulated (including as to capital) should not be segregated within that regulated deposit-taking institution, and such institution should have the ability to treat any such deposits as a regular deposit, which constitutes a deposit liability of a commercial banking institution, provided that there is clear disclosure to relevant clients that their cash will be treated as a deposit liability. The recommendations in Chapter 7, therefore, should not apply in such circumstances.

- Where a CASP has issued a fiat-backed stablecoin, and the fiat cash that acts as the reserve is held at an appropriately regulated deposit-taking institution, that cash should also not be segregated within that regulated deposit-taking institution.

- Client assets not treated as deposit liabilities or for which the CASP otherwise is not permitted to reuse for its own purposes should not be recorded on the CASP's balance sheet merely because the assets make use of DLT. We note that contrary treatment in certain jurisdictions (*e.g.*, SEC Staff Accounting Bulletin 121) has unduly inhibited the ability for traditional financial institutions to provide custodial services for crypto-assets due to the issues posed by such accounting treatment when intersecting with capital and other

[54] In this regard, we note that other industry groups have commented on recent regulatory proposals with respect to custody issues. We encourage IOSCO and its members to review these comments in connection with the finalization of the CDA Recommendations. *See, e.g.*, SIFMA, Comment on Proposed SEC Rule re: Safeguarding Advisory Client Assets (May 8, 2023), *available at* https://www.sifma.org/wp-content/uploads/2023/05/Safeguarding-Advisory-Client-Assets.pdf. We also noted that other industry groups have provided responses to this consultation, and we encourage IOSCO and its members to review those comments in connection with the finalization of the CDA Recommendations as well. *See, e.g.*, Comment of the Association of Global Custodians on OICU-IOSCO Policy Recommendations for Crypto and Digital Asset Markets Consultation Report.

prudential regulations, which tends to discourage more comprehensively regulated institutions from providing these services.

<u>Question 15</u>:

<u>(a)</u> Should the Recommendations in Chapter 7 address the manner in which the customer crypto-assets should be held?

The Recommendations should acknowledge that a blanket approach is not appropriate with respect to custody regulations. Rather, custody regulations should seek to ensure client asset protection by requiring controls that are commensurate with the complexity and risk of the service being provided.

Furthermore, consistent with our comments provided in the letter above, the Recommendations should account for the fact that many CASPs are already subject to custody regulations and should not impose additional or different requirements in relation to crypto-asset custody that do not apply to traditional assets where the use of DLT does not necessarily introduce new risks or other issues (*e.g.*, disclosures relating to use of sub-custodians or omnibus custody).

Importantly, and as noted above, the Recommendations should not affect the way that client cash is held (*i.e.*, as part of liabilities), by the CASP's fiat cash custodians that are regulated deposit-taking institutions.

<u>(b)</u> How should the Recommendations in Chapter 7 address, in the context of custody of customer crypto-assets, new technological and other developments regarding safeguarding of customer crypto-assets?

As detailed above, the Recommendations should not be overly prescriptive with respect to new technology and other policy developments, given the rapidly evolving technology in this space. For example, the Recommendations should acknowledge the use of "private keys" and different types of "wallets" in the crypto-asset context.[55]

The Recommendations also should not be more prescriptive than those that apply in the traditional financial sector, consistent with the "same activities, same risk, same regulatory outcomes" approach; our proposed revisions to Recommendation 14 are intended to reflect this position (*e.g.*, by removing heightened disclosure requirements with respect to sub-custodians or omnibus custody, which are not required in other settings).

Furthermore, the Recommendations should acknowledge the differences amongst crypto-assets; please see our comments regarding the GFMA Taxonomy provided in the letter above.

Additionally, crypto-asset markets can make use of smart contracts to facilitate safekeeping or transfer of digital assets in ways that should be treated more like technology or communication

[55] *See, e.g.*, GFMA Whitepaper at 76-78.

protocols, which may be used by financial services providers, than as its own provision of financial services. One example of this is the creation and use of smart contracts to enable interoperability between assets created by different technology stacks (*e.g.*, cross-chain bridges). In this regard, technology firms or developer communities that are not regulated financial industry participants can be key drivers to the development or governance of this technology. In order to promote regulatory clarity, such firms should not be in scope of financial services licensing or similar requirements to the extent they are merely part of the broader community of contributors to the technology as opposed to controlling its operation. Of course, where a regulated financial institution utilizes technology such as a cross-chain bridge, the relevant regulator can engage in connection with its supervisory powers (*e.g.*, as to operational resilience). We would also expect such a financial institution to conduct the appropriate due diligence on any new technology product before implementing its use (and for clients, particularly institutional ones, to require such diligence, as well as other standard protections).

Finally, given that many crypto-assets operate using private-public cryptographic keys (which can be thought of as strings of code that provide access to a particular crypto-asset and are, therefore, important to keep safe and appropriately custodied), in cases where such a crypto-asset is not itself a regulated financial product (and does not represent an interest in regulated financial product), these keys should be out of scope for any financial data localization requirements. This approach would be necessary given the global nature of crypto-asset markets and to encourage the responsible development of this technology.

<u>(c)</u> What safeguards should a CASP put in place to ensure that they maintain accurate books and records of clients' crypto-assets held in custody at all times, including information held both on and off-chain?

Consistent with the approach taken in traditional financial markets, CASPs should have policies and procedures in place, including as relevant, internal and external audit functions, to ensure the maintenance of accurate books and records in compliance with applicable regulation. Such policies and procedures should account for new technologies and incorporate best practices that develop with respect to DLT.

As applicable, CASPs should also conduct frequent reconciliations between their internal books and records and the record as reflected on the relevant DLT. CASPs should have policies and procedures in place to identify and resolve any discrepancies, and regulators should, consistent with the approach taken in traditional financial markets, require reporting of significant discrepancies. In order to facilitate such reconciliations, regulators should engage with market participants to understand evolving best practices with respect to settlement finality in the context of on-chain DLT transfers. For example, while in some cases, unless and until a transfer of a crypto-asset has been reported on the consensus state of a blockchain, settlement of an on-chain transfer is not yet legally authoritative, industry practices with respect to determining consensus states and exceptions continue to evolve (*e.g.*, 6 blocks for bitcoin, a ~15 minutes lapse for

Ethereum or a "Single Slot Finality" epoch (~6.4 minutes) in the future,[56] and Layer 2 point of deemed settlement finality). By permitting firms to rely on public blockchain records where reasonable steps are taken to follow best practices, regulators can help foster responsible innovation.

***(d)* Should the Recommendations in Chapter 7 include a requirement for CASPs to have procedures in place for fair and reliable valuation of crypto-assets held in custody? If so, please explain why.**

To the extent a jurisdiction requires a regulated entity to have procedures in place for fair and reliable valuation of traditional assets held in custody, such requirements should apply, in the same manner, to crypto-assets held in custody (with the recognition that, for many crypto-assets, just like traditional financial assets such as currencies or bonds that trade on multiple venues and/or over the counter, there may not be a single market price to use as a basis for valuation, and so "fair and reliable" valuation procedures will vary among crypto-assets). The requirements may differ based on the particular service provided by the CASP (for example, for some CASPs, providing valuations might be the core offering, while, for others, it may be ancillary; the rules should recognize these differences).

***Question 16*: Should the Recommendations address particular safeguards that a CASP should put in place? If so, please provide examples**

Recommendation 16 suggests that regulators should consider whether and how a CASP can compensate its clients under applicable law, in the event of theft or loss of client assets.

A foundational building block to address this objective is for applicable regulations to provide for clear limitations on liability for CASPs providing custodial services. Specifically: (1) a CASP acting as custodian should not be liable for losses incurred due to events outside of the CASP's control; (2) any compensation for loss should be capped at the lost asset's market value at the time of the loss; and (3) CASPs and institutional clients should be able to negotiate limitations on liability, subject to appropriate minimum requirements.

With regard to requirements for CASPs to hold sufficient assets to compensate clients, existing operational risk capital requirements should be deemed sufficient for this purpose; additional own funds or guarantee obligations should not be imposed merely because of the use of DLT. Regulators should encourage the development and implementation of insurance products and standards for crypto-assets as well.

Separately, requirements regarding custody disclosures (and more generally) should be allowed to vary based on the type of customer. For example, the Recommendations suggest that "non-technical" risk disclosures are preferable; while that might be true for retail customers, institutional customers may prefer to receive more technical disclosures.

[56] *See* https://ethereum.org/en/roadmap/single-slot-finality/.

We have also included below some suggested changes to the text of the Recommendations 12 through 15.

Recommendation 12 (Overarching Custody Recommendation): Regulators should apply the IOSCO Recommendations Regarding the Protection of Client Assets[57] *when considering the application of existing frameworks, or New Frameworks, covering CASPs that hold or safeguard Client Assets, excluding deposit liabilities of banks that are appropriately regulated (including as to capital), while also taking into account the particular custody services provided by a CASP.*

Recommendation 13 (Segregation and Handling of Client Monies and Assets): Regulators should require a CASP to place Client Assets, excluding deposit liabilities of banks that are appropriately regulated (including as to capital), in trust, or to otherwise segregate them from the CASP's proprietary assets.

Recommendation 14 (Disclosure of Custody and Safekeeping Arrangements): Regulators should require a CASP to disclose, as relevant and taking into account whether the client is a retail client or an institutional or professional client, in clear, concise and non-technical language to clients:

- *How Client Assets are held, and the arrangements for safeguarding these assets and/or their private keys; and~~.~~*
- ~~*the use (if any) of an independent custodian, sub-custodian or related party custodian;*~~
- ~~*the extent to which Client Assets are aggregated or pooled within omnibus client accounts, the rights of individual clients with respect to the aggregated or pooled assets, and the risks of loss arising from any pooling or aggregating activities;*~~
- *Risks arising from the CASP's handling or moving of Client Assets, whether directly or indirectly, such as through a cross-chain bridge.* ~~*; and*~~
- ~~*Full and accurate information on the obligations and responsibilities of a CASP with respect to the use of Client Assets, as well as private keys, including the terms for their restitution, and on the risks involved.*~~

Recommendation 15 (Client Asset Reconciliation and Independent Assurance): Regulators should require a CASP, as relevant based on the services provided by the CASP, to have systems, policies, and procedures to conduct regular and frequent reconciliations of Client Assets subject to appropriate independent assurance.

Recommendation 16 (Securing Client Money and Assets): Regulators should require a CASP, as relevant based on the services provided by the CASP, to adopt appropriate systems, policies and procedures to mitigate the risk of loss, theft or inaccessibility of Client Assets. Regulations should take into account existing operational risk capital requirements and provide for limitations on liability, including that: (1) a CASP acting as custodian should not be liable for losses incurred due to events outside of the CASP's control; (2) any compensation for loss should be capped at the market value of the lost crypto-asset at the time of the loss; and (3) CASPs and professional or

[57] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD436.pdf.

institutional clients should be able to negotiate limitations on liability, subject to appropriate minimum requirements.

Chapter 8: Recommendation to Address Operational and Technological Risks

***Question 17**: Are there additional or unique technology/cyber/operational risks related to crypto-assets and the use of DLT which CASPs should take into account? If so, please explain.*

Regulators should apply existing regulatory regimes with respect to operational risk management, including systems testing, operational resilience, and business continuity. Operational risk management programs should take into account circumstances where DLT introduces unique characteristics (*e.g.*, allowing for pseudonymity or incorporating the use of a public validator network), though we do not believe that new regulatory frameworks are needed to account for DLT. Furthermore, to the extent a CASP would otherwise be subject to the Principles for Financial Market Infrastructures, it should comply with those principles and any other regulations that apply to critical or systemically important service providers.[58]

***Question 18**: Are there particular ways that CASPs should evaluate these risks and communicate these risks to retail investors? If so, please explain*

CASPs should be required to evaluate operational and technological risks and communicate those risks (to retail and professional or institutional investors) in a manner consistent with how regulated entities evaluate and communicate risks with respect to the use of any new technology in the traditional financial markets.

We have also included below some suggested changes to the text of the Recommendation 17.

Recommendation 17 (Management and Disclosure of Operational and Technological Risks): Regulators should require a CASP to comply with requirements pertaining to operational and technology risk and resilience in accordance with IOSCO's Recommendations and Standards. Regulators should require a CASP to disclose, taking into account whether the client is a retail client or an institutional or professional client, in a clear, concise and non-technical manner, all material sources of operational and technological risks and have appropriate risk management frameworks (e.g. people, processes, systems and controls) in place to manage and mitigate such risks.

Chapter 9: Retail Distribution Recommendation

***Question 19**: What other point of sale / distribution safeguards should be adopted when services are offered to retail investors?*

[58] Principles for financial market infrastructures (Apr. 16, 2012), *available at* https://www.bis.org/cpmi/publ/d101.htm; *see also* Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Dec. 2022), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN.

The commentary accompanying Recommendation 18 describes a specific standard for suitability assessments (specifically, that they be "well constructed and robust and do not give clients the false impression that they sufficiently understand the operations of crypto-asset markets and the related risks, when this is not the case"). We note that this standard diverges from existing suitability requirements, such as those found in FINRA Rule 2111. Existing suitability requirements also tend to apply to a particular type of investment service provided rather than the specific type of asset included in the service. At least with respect to traditional assets using DLT, suitability standards should be consistent with those applicable to traditional financial markets.

We have also included below some suggested changes to the text of the Recommendation 18.

Recommendation 18 (Retail Client Appropriateness and Disclosure): Regulators should require a CASP, to operate in a manner consistent with IOSCO's Standards regarding interactions and dealings with retail clients. Regulators should require a CASP to implement adequate systems, policies and procedures, and disclosure in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client, consistent with the suitability requirements that apply with respect to traditional financial products and services.

Question 20: Should regulators take steps to restrict advertisements and endorsements promoting crypto-assets? If so, what limitations should be considered?

Existing advertising and marketing requirements that apply to traditional financial markets and products (*e.g.*, FINRA Rule 2210) are adequate and should apply with respect to crypto-asset promotions as well.

Chapter 10: Box Text on Stablecoins

Question 21: Are there additional features of stablecoins which should be considered under Chapter 10? If so, please explain.

We think it is important to distinguish among different types of stablecoins. As drafted, CDA Recommendations define "stablecoins" broadly[59] and would apply the Recommendations to all stablecoins. As we have noted elsewhere, to ensure clarity, certain types of digital tokens that are designed to maintain stable value but that are otherwise fundamentally different from stablecoins should be excluded from the stablecoin definition. For example, the proposed treatment of stablecoins should not apply to tokenized commercial bank money or FMI tokens, as described in GFMA's Taxonomy. Instead, such assets should be treated as, and subject to existing regulations regarding, bank deposits. Additionally, central bank digital currencies, FMI tokens, settlement tokens or non-fungible tokens should not be included in the stablecoin definition.[60] These types

[59] CDA Recommendations at 41 (adopting the FSB's definition of stablecoin: "a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets").

[60] *See* GFMA FSB Response, *supra* note 4, at 17.

of assets do not give rise to the issues that seem to be central to IOSCO’s concerns (*e.g.*, the sufficiency of reserve assets; algorithmic backing; use in crypto-asset trading pairs, etc.).[61]

[61] *See also supra* note 15.

Annex B

Annex 1: GFMA Proposed Approach for the Classification and Understanding of Digital Assets

Initial Proposed Approach for the Classification and Understanding of Digital Assets[62]

The Global Financial Markets Association (GFMA) developed the following approach to classification of digital-assets to support our response to the Basel Committee on Banking Supervision (BCBS) discussion paper on **'Designing a Prudential Treatment for Crypto-Assets'[63] and** FSBs recent consultation on the **"Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets".** The approach reflects the principle that the treatment of digital-assets should be underpinned by clear methodology for identifying different types of digital-assets' risk which will allow for tailored regulatory treatment, as appropriate.

We believe this provides an initial basis for a taxonomy and it is key that there is close engagement between the industry and the regulatory community on this topic. We therefore recommend a joint industry-regulatory task force is formed to urgently develop a global taxonomy as a priority in 2023.

Approach to classification and understanding of digital assets

Broadly, digital assets may serve a variety of economic functions, such as an agent for payments[64], a vehicle for investment or trading[65], or a utility to access other goods or services[66]. Within those functions, when those assets have the characteristics of existing regulated instruments, a specific regulatory framework may apply. However, given the features of digital-assets, other key attributes beyond economic function, may need to be taken into consideration by regulators in order to classify those assets and determine what regulations should apply, if any (similar to how frameworks such as those that are leveraged for classifying a security/financial instrument function today).

For this initial taxonomy proposal[67] we focused on defining features of digital-assets such as:

[62] As discussed in our Note to the Reader, we believe that 'digital-assets' is a much more appropriate term when discussing DLT based assets in the general sense. However, we would reiterate our initial point that a global taxonomy is urgently needed. We would note that when we discuss digital assets that this does also include fiat deposit accounts where the transfer of ownership is accomplished via blockchain or DLT.

[63] GFMA Response to BCBS Discussion Paper on the Prudential Treatment for Crypto-Assets.

[64] Payment tokens may also be referred to as exchange tokens in some jurisdictions. Key uses may include, the crypto-asset being held and transferred primarily for the purposes of buying or selling other assets or being used as a store of value.

[65] Security/ Investment/Financial instrument tokens provide entitlement to proceeds or a right to vote and could also meet the characteristics or definition of a financial instrument or equivalent regulatory classification.

[66] Crypto-assets used as a means of accessing a DLT platform and/or a medium of exchange for the provision of goods and services provided on the DLT platform, and does not have value or application, outside of the DLT platform on which it was issued (Note that the crypto -asset may be used as a means for data and database management, data recordation, or other bookkeeping or recordkeeping activity. As these do not constitute financial instruments, they are intentionally excluded here.)

[67] This approach has not been formally endorsed by all GFMA members and is intended as a basis for discussion.

- **Issuer** (e.g., central bank)
- **Mechanism or structure underlying the asset value** (e.g., pegged to or in reference to an underlying asset or access to a network product or service)
- **Rights conferred** (e.g., entitlement to cash flows, redemption rights, voting)
- **Nature of the claim** (e.g., claim on an issuer or claim on an underlying asset)

There are additional features that should be assessed against each type of digital-asset to help differentiate and evaluate the risk, including types of users/holders (e.g., retail versus wholesale), **systemic importance,** and if an **asset is linked to a real or off-chain asset,** who or what **type of entity has Custody of that asset,** if any.

Other features that we recommend be considered for a future global taxonomy is the type of network upon which the digital asset exists. There are various configurations of DLTs, each with varying levels of privacy, governance and control. These are set out below:

- **Private-permissioned (e.g., R3 Corda):** Private-permissioned networks are characterized by a centralized authority that can control **access to the network** (private) and **actors that can perform actions on the network** (permissioned). Private networks enable a comparable model to existing infrastructure used by capital markets today, with control over all network layers, and their defining characteristics mean existing legal, regulatory and institutional risk management frameworks (operational risk and cyber resilience frameworks) can be applied.
- **Public-permissioned (e.g., Corda Network):** Public-permissioned networks are characterized by allowing **public access to the network** and a centralized authority to control **actors that can perform actions on the network** (permissioned). Though public-permissioned distributed networks mark a step away from the tight central control of private networks, they also operate as closed networks with centralization retained over key network attributes. Therefore, like private networks, the same legal, regulatory, and institutional risk-management frameworks also provide a sufficient basis to govern these networks, including differentiated considerations around cybersecurity and impacts on operational resilience, and KYC/AML/CFT compliance.
- **Public-permissionless (e.g., Ethereum):** Public-permissionless networks allow unrestricted access to the network and allow anyone to perform actions on the network by default. These publicly available distributed ledger networks have defining characteristics, such as decentralization, pseudonymity, and large-scale user bases, that are different to private-permissioned and public-permissioned networks.

Further to this distinction, digital assets can be subdivided into characteristic types:

- **Fungible:** interchangeable and divisible – like securities, cash, or commodities
- **Non-Fungible:** unique and indivisible – like real estate, fine art, and other nonfinancial assets
- **Digital Only or Real World:** accessed via a centralized bridge that relies on a service provider

Both of these distinctions should also be part of the 'type' that digital assets can belong to in a global taxonomy. Many digital assets have functions and features spanning more than one of the categories or may not even be contemplated at this time[68]

These types of digital assets may have characteristics that enable their use for more than one purpose (means of payment or investment) at any single point in the lifecycle of the asset or have characteristics that change during the course of their lifecycle. Further consideration should be given to these types of assets as well as when and how the rules should apply to them. The GFMA would encourage an approach that is agile and remains robust, providing the market clarity while also allowing innovation as market structures develop, uses evolve, and technology changes, or new assets are created.

While we have used the term 'digital-asset,' as the overarching category to group together a number of instruments, not all the categories (and associated uses and attributes) should be treated as instruments for which a new financial regulatory framework is necessary or appropriate. A robust regulatory framework (including customer/investor protection safeguards) may already exist for the instruments or activity represented by the 'digital-asset.'

We would reiterate that the proposal below is intended to be an initial starting point for a classification of digital assets. It is designed to help regulators evaluate which types of regulations should apply to which type of assets. We note however that as these assets evolve and potentially new ones are created, this classification may need to be updated over time. We would still encourage that a global taxonomy be developed. This global taxonomy should be comprehensive, but also have the ability to be reviewed and adapt with time and new innovations.

Types of Digital Assets[69, 70]

Value-Stable Digital Assets

1. Tokenized Commercial Bank Money[71]

- Digital tokens reflecting a deposit ownership claim reflected on DLT for a fixed amount of fiat money denominated in a single currency by the token-holder against the token issuing bank or other similarly highly regulated depository institution. It may or may not pay interest.

[68] As the crypto-asset market evolves and the understanding of uses matures, additional uses beyond those identified as payment, investment, or utility may need to be addressed or identified.

[69] GFMA also notes that the term 'coin' and 'token' are synonymously leveraged below and are not intending to insinuate differences between the two terms.

[70] Some of those instruments may meet the 'e-money' criteria in those jurisdictions where that regulatory classification exists and be classified as such for regulatory purposes.

[71] Note: Deposits recorded via DLT may not be considered true digital assets as they do not create a new asset class with separate intrinsic value from the fiat currency they represent. However, we have included this to be responsive to varying definitions of digital asset under consideration, and to comprehensively articulate when the use of distributed ledger technology would not require new regulatory treatment, but would be governed by an existing regulatory framework.

2. **Financial Market Infrastructure (FMI) Tokens (e.g., USC)**

    - Digital tokens representing a claim on an FMI for a fixed amount of fiat money denominated in a single currency by the token-holder, fully collateralized by reserves held at a central bank or deposits held at a commercial bank. It may or may not pay interest.

3. **Wholesale Central Bank Digital Currencies (wCBDC[72], none launched)**

    - Specialized, limited purpose digital tokens representing a claim on a central bank for a fixed amount of fiat money denominated in a single currency, designed for specific use by wholesale market participants who have central bank account access. It may or may not pay interest.

4. **Stablecoins (e.g., USDC):** Tokens designed to minimize price fluctuations relative or in reference to other asset(s) which are not issued by a central bank, FMI, bank, credit institution or highly-regulated depository institution. May represent a claim on the issuing entity, if any, and/or the underlying assets. There are two types of stablecoins.

    - Asset Linked Digital-Asset: value may be fixed or variable and in reference to individual structures or include a combination of:

        - Fiat currency linked (e.g., Tether, Paxos, USDC)

        - Other real asset linked (e.g., Sendgold)

        - Digital asset linked (e.g., Maker)

    - Algorithmic Digital-Asset: Typically, not linked to any underlying assets and each token can be pegged to a price level or a unit maintained through buying, selling or exchange among assets or some other pre-determined mechanism. To meet the standard defined here, an algorithmic digital asset must be pegged to assets that are highly liquid and hold intrinsic value

DLT-based Securities[73]

- **Tokenized Security (e.g., UBS AG's digital bond dual listed on Swiss SIX and SDX):** Token that represents on DLT infrastructure underlying securities/financial instruments issued on a different platform (e.g., a traditional CSD, registrar, etc.), where such representation itself satisfies the definition of a security/financial instrument under local law.

- **Security Token (e.g., World Bank's "Blockchain Bond"):** Token issued solely on DLT infrastructure that satisfies the applicable regulatory definition of a security or financial instrument under local law

Cryptocurrencies

- Digital representations of value with no redemption rights against a central party and may function within the community (enabled through peer-to-peer networks) of its users as a medium of exchange, unit of account or store of value, without having legal tender status. They may also act as an incentive

[72] CBDC can rely on non-DLT/blockchain technology, this taxonomy is intending to capture only those leveraging DLT/blockchain technology.

[73] This category encompasses different regulated instruments from a legal perspective, which may attract different regulatory treatment amongst themselves and across jurisdictions.

mechanism and/or facilitate functions performed on the network they are created in; their value is driven by market supply/demand therein.

Settlement Token

- Representation on DLT or blockchain infrastructure of underlying traditional securities/financial instruments issued on a different platform (e.g., a traditional CSD, registrar, etc.) where such representation itself does not satisfy the definition of a security or financial instrument under local law and is used solely to transfer or record ownership or perform other mid/back-office functions (e.g., collateral transfer, recording of ownership)

Utility Token

- A means of accessing a DLT or blockchain platform and/or a medium of exchange which participants on that platform may use for the provision of goods and services provided on that platform (e.g. loyalty rewards pro- grams/systems, gift card rewards, credit points that are only usable within the DLT or blockchain platform, memory and network server space, and other utilities- based value); or

- Tokens that are not native to the underlying network but are used for accessing applications that are built on top of another DLT or blockchain infrastructure platform (dApp)

Other Crypto-Assets (not structured as value-stable crypto-assets)

- Representation on DLT or blockchain infrastructure of ownership in tangible or intangible underlying assets or of certain rights in those assets (such as interest, e.g., loans), which are not securities or financial instruments (e.g., real estate, art, intellectual property rights, precious metals, grains, or non-fungible assets that only exist in digital form on a DLT network); they may represent a claim on the issuing entity or the underlying assets.