International Organization of Securities Commissions (IOSCO): Policy Recommendations for Crypto and Digital Asset Markets

Public Comment on IOSCO's Consultation Report by the Digital Currencies Governance Group

About DCGG

Digital Currencies Governance Group (DCGG) is a trade association that represents digital assets issuers and service providers in the United Kingdom and the European Union. Our mission is to facilitate an open dialogue and encourage communication between policymakers and digital asset experts to support the design of a sound and proportionate regulatory framework that ensures safety for all market participants. Our Members include Tether - currently the largest stablecoin issuer worldwide, Ledger - a leading technology service provider for self-custody, Bitfinex - a crypto-assets exchange, ZKValidator (ZKV) - a leading proof-of-stake validator, and Iden3 - a solutions provider for self-sovereign identity management. Our team of former government officials, lawyers, and cryptoasset experts regularly engage with policy-makers and regulators both at the national and international level. For any general enquiries or to request further information, please do reach out to info@dcgg.eu.

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.

DCGG and its members agree with the set of activities and services covered by the IOSCO Recommendation 1, and we see the proposals are exhaustive enough at this stage, given the nascent nature of the crypto-asset industry and emerging utilities and applications.

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?

DCGG and its members are supportive of outcomes-based regulatory principles to be followed by IOSCO members in order to safeguard investor protection and market integrity. However, to ensure effectiveness in applying an outcomes-based approach, the steps taken would require:

- In-depth understanding of different business models within the sector.
- Consideration of how best to adapt existing or bespoke regulations to take into account the different business models in the sector, as this is essential for proportionality.

- Consideration of risk levels of different products and services, e.g., algorithmic stablecoins vs. fiat stablecoins, where the former carries a significantly higher level of risk, or software vs. hardware wallets, whereby the latter is understood to provide a higher level of security for the end-user by default.
- Establishing a clear set of definitions that can be easily updated to include emerging business models that ensure legal certainty for the sector.
- Ongoing cooperation with the crypto-asset industry to effectively achieve the set outcomes, e.g., sandboxes, public-private partnerships.

In our view, taking this direction might be more appropriate to allow for the innovation in the sector, while still meeting the objective to ensure investor protection, market stability and integrity across IOSCO members.

As part of the process of gaining a more holistic understanding of the sector, we would like to highlight that crypto-asset markets should be assessed through the particular use-cases of different products and services, rather than be subject to a generalised rulebook based on underlying technology. In particular, Chapter 1 of this consultation document references "crypto-assets are, or behave like substitutes for, regulated financial instruments". In the case where this statement in its current format informs regulatory decision-making, in our view, certain crypto-assets could falsely or prematurely fall in scope of the categorisation of financial instruments regulated by existing rulebooks. In order to avoid legal uncertainty, we recommend that regulators assess crypto-asset features and applications in detail to ensure a certain crypto-asset does or does not assume a financial instrument role.

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?

DCGG and its members understand IOSCO's concerns around potential conflicts of interest arising from vertically integrated CASP activities in light of last year's FTX collapse. From our perspective, the objectives communicated in Recommendation 2 and the examples outlined in this consultation document adequately reflect potential conflicts of interest between certain CASP activities (order-matching vis-a-vis market making), however for the purposes of legal certainty, we would welcome further detail and guidance from IOSCO as to which other activities or combination of activities are permissible and which could be flagged as potentially problematic by the regulator.

Question 4: 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?

From DCGG's perspective, conflicts of interest should be mitigated, as a main starting point, internally by CASPs, with the help of lists of recommendations and practices to potentially implement, without enforcing a regulatory requirement, to allow the industry to maintain its operational stability and the integrity of its market. For example, effective practices could be:

- **Establishing a code of conduct**: A code of conduct can set out the principles that CASPs should follow in order to avoid conflicts of interest. This could include principles such as transparency, fairness, and independence.
- **Ensuring adequate training**: CASPs should ensure that their employees are adequately trained on how to identify and manage conflicts of interest. This training should cover the specific risks that arise in the crypto asset industry.
- **Having an independent oversight body**: An independent oversight body can be established to monitor the activities of CASPs and to investigate allegations of conflicts of interest. This can help to ensure that CASPs are complying with the relevant rules and regulations.

On the other hand, methods such as separation of activities in separate entities and prohibition of conflicts should be used only in cases where the aforementioned practices do not deliver the desired results, and excessive risk has been identified, or if there is evidence to point out that conflicts of interest have been intentionally caused. Importantly, outside of the aforementioned scenarios, measures such as restriction of combining certain crypto-asset activities within a group of affiliated entities would not abide by the principle of proportionality and would very negatively impact the growth and operations of service providers if applied across the sector. Overall, DCGG would encourage CASPs to follow sound internal governance practices (e.g., establishing a code of conduct, ensuring adequate staff training, and having an independent oversight body) and for specific risk mitigation measures such as disclosure of potential conflicts of interest to be enforced to promote consumer protection.

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

In our view, the proposed disclosure requirements are reasonable and would be effective in conflict of interest risk mitigation.

Chapter 3
Recommendations on Order Handling and Trade Disclosures (Trading Intermediaries vs Market Operators)

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?

IOSCO's proposed recommendations outline the need for consistency between existing regulations for exchanges and brokers, and the approach to the crypto-asset market. This consistency should be outcomes-based, and ideally achieved through new frameworks.

We believe that Recommendations 4 and 5, which focus on CASPs operating as trading intermediaries, will be beneficial for both trading intermediaries and market operators. The fair treatment disclosure requirements outlined in Chapter 5 are comprehensive enough to provide crypto operators with the legal clarity they need to comply effectively with regulatory obligations.

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.

Market operators and trading intermediaries are important actors in the crypto-asset ecosystem. From the perspective of the market, we do not see specific concerns with regard to CASPs engaging in both activities, as this allows diversity in the products and services offered and catering to specific needs of the end-user. Therefore, we believe that CASPs should not be limited in offering different services, such as the ones outlined under Chapter 3, as long as they follow effective governance protocols (as outlined in our response to question 4), and also as long as this is clearly disclosed to customers in order to facilitate informed decision-making and ensure there is clear understanding of the specificities of the services provided.

Furthermore, we encourage cooperation between regulators and crypto operators, and believe it would be most efficient and appropriate for a government or regulatory authority, or another independent body, to work with CASPs to establish a shared list of requirements for disclosure. This would support fair and objective requirements that would allow for effective risk mitigation and consumer protection.

Question 8: Given many crypto-asset transactions occur “off-chain” how would respondents propose for CASPs to identify and disclose all pre- and post-trade “off-chain” transactions?

In order to ensure order handling and disclosures in the on- and off-chain context is robust enough, DCGG and its members recommend the identification and disclosure of pre- and post-trade off-chain transactions to be done through tools such as real-time logging of order book activity, depth charts and post trade recording on the website of the trading platform. This is a very effective and transparent manner for disclosing off-chain transactions to customers, thus facilitating informed investor decisions. To supplement the use of these tools and metrics, we support disclosures, e.g. through a specific set of terms and conditions, of the risks involved in participating in such transactions, to ensure transparent communication with users. This way, based on their risk appetite, users would be able to decide what types of transactions to partake in.

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

Question 9: Will the proposed listing/delisting disclosures 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?

Based on the provisions outlined in Chapter 4, we foresee the potential of these proposals to be effective for robust public disclosure. Yet, DCGG and its members would like to highlight with regard to the proposed obligation for CASPs to disclose the same information about non-identifiable crypto-asset issuers as they do for identifiable issuers, that such an expectation could be very onerous for crypto-asset operators. While we agree with the importance of the proposed disclosures for informed decision-making and investor protection, some pieces of information (e.g., full information about the issuer and its business, including audited financial statements, and information about the issuer's management team) could be very challenging or even impossible for CASPs to find, identify and disclose for the purposes of compliance with this Recommendation. In this case, regulators should exercise a more granular, case-by-case approach in order to make clear that disclosures can be partial when the issuing entity is not identifiable and thus prevent excessive administrative burden to be placed on CASPs.

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.

DCGG and its members would welcome further clarity on how regulators would understand and issue rules governing a CASP's 'proprietary crypto-asset' and how 'material interest' is determined with regard to primary market activity under Recommendation 7 for the purposes of legal clarity for industry participants. For instance, CASPs could issue and list their own 'exchange tokens', 'exchange crypto-assets' or crypto-assets with which the platform is affiliated and which have the utility of granting benefits to token holders within the ecosystem of the CASP. With this in mind, these play an important part of the overarching crypto sector and facilitate important market activities. Therefore, DCGG and its members do not believe limitations or prohibitions should be applied in this case, rather we recommend a proportionate treatment which would entail that such tokens fall in line with the disclosure and issuing processes applied to other market participants (as outlined in previous chapters), allowing the user to make an informed decision on whether to interact, transact and generally invest in such tokens. From our perspective, these standards and recommendations are comprehensive enough to mitigate the risks outlined by IOSCO, and the suggested restrictions and prohibitions run the risk of inadequately addressing this strand of the industry in a way which will stifle its development.

In general, providing further guidance on what is considered a proprietary crypto-asset in this context would be a crucial distinction to make clear and for potential regulatory risk mitigation measures to be proportionate to the level of risk, which also needs to be objectively assessed.

Chapter 5
Recommendations to Address Abusive Behaviors

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?

In DCGG's view, the offences outlined in Chapter 5 are exhaustive and adequately reflect the realities and risk levels in crypto-asset markets. The prevention of the proposed offences would therefore be effective in tackling market abuse and fraudulent practices.

b) any novel offences, or behaviors, specific to crypto-assets that are not present in traditional financial markets? If so, please explain.

Proportionality is essential to enforcing a strong risk mitigation framework to address the divergent scope of abusive behaviours within a market, and we encourage regulators not to perceive the crypto-asset industry as inherently riskier than traditional finance, including by working under the assumption that crypto products and services pose sector-specific risks, when in reality all risks observed in crypto already exist in the world of traditional finance in some form or another. We therefore do not believe that any novel offences or behaviours that cannot be mitigated can be expected to occur, as long as operators are providing crypto-asset services under a regulatory rulebook that grants the necessary legal certainty and promotes innovation and development of economic activity.

Question 12: 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.

The proposed market surveillance requirements sufficiently address market abuse risks, which in DCGG's view, are similar across traditional finance and crypto asset markets, despite the environment and context (e.g., on the Blockchain) operations occur. Moreover, DCGG and its members believe that CASPs are very well-positioned, both in the on- and off-chain context, to tackle market abuse risks due to the underlying Blockchain technology and its benefits of transparency, immutability and traceability, which are unique to the sector. DLT allows for implementing sophisticated internal controls to tackle fraud, market manipulation, money laundering, identification of illicit actors, filing of suspicious

transactions reports and cooperation with law enforcement as soon as suspicious activity is flagged., In some cases, it also allows centralised control and immediate freezing of assets, These benefits coupled with the surveillance requirements outlined in this chapter would facilitate effective mitigation of market abuse risks within the sector.

Finally, we support the rationale outlined in Chapter 5 that regulators should take a proportionate approach to market surveillance of CASPs, based on their nature, scale and complexity of the business and service provision. We encourage a case-by-case assessment, close cooperation and ongoing communication with the industry, and avoiding the enforcement of a generalised approach to the requirements for crypto operators.

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?

DCGG and its members understand the need for reducing the risk of regulatory arbitrage in light of the cross-border nature of crypto-asset activities, and support the implementation of a harmonised information sharing system between competent authorities at the national and international levels. To strengthen cross-border cooperation, we believe information exchange, joint investigation and enforcement would lead to more effective protection of financial markets from cross-border fraudulent activity.

Given the complexities of enforcement at a cross-border level, in our view competent authorities should consider multilateral cooperation beyond the regulatory level (Recommendation 11) and engage in ongoing communication and partnerships with CASPs, as well as industry experts, in order to ensure enforcement and oversight are proportionate to the realities of the sector. For example, as stated in question 12, CASPs have in place the resources to share information through suspicious transaction reports, blockchain analytics and market observation forms to inform a better understanding of the ecosystem and tackle illicit activities.

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?

The Recommendations under Chapter 7 comprehensively encompass the specific considerations and implications of custodial activity and the internal controls and provisions

necessary to protect investors' assets. Nevertheless, we would like to point out that only operators that have access to clients' assets and keys should be subject to these provisions, as this is essentially what the custodial nature of a service entails. It should not include technical service providers that merely provide the cold hardware to enable self-custody for their users, which means that the user is responsible for safeguarding the assets. We would welcome further clarity to ensure that these solutions providers will not be subject to regulatory requirements, given they have no access or control over investors' assets. Finally, we support an explicit distinction between such technological providers and what is regarded in this consultation document as a 'cold wallet'.

Question 15:

(a) Should the Recommendations in Chapter 7 address the manner in which the customer cryptoassets should be held?

From an industry perspective and for the purposes of legal certainty, it would be useful for the Recommendations to outline the regulatory expectations for the holding of user funds in order to facilitate compliance for market participants which have access or control over customers' assets. We believe that regulators should be recommended to consider the unique operating model inherent in the underlying blockchain technology that underpins the industry, and the importance this has on defining appropriately contextualised recommendations regarding segregation of assets. For example, the primary method through which most crypto-asset platforms generate revenue is through fees taken on the trading activity of their users. Fees generated from customer assets would by definition become 'company funds' at that point implying the need for those funds to be transferred away from a wallet holding customer funds, to one of the company's. Such a transaction would be an on-chain transaction, and result in blockchain fees, which would significantly reduce any profit made from fees generated, and risk reducing the financial stability of platforms. This is one example of various practical implications that may arise with requirements pertaining to segregation, and why it is therefore crucial that recommendations and principles defined on this topic reflect the unique operating model of the industry and its underlying technology.

(b) 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?

To ensure the regulatory approach is future-proof, a technology-neutral and pro-innovation manner of addressing emerging developments in the custody space is encouraged.

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

To ensure consistency with the treatment of other crypto operators, in our view, the Recommendations should outline specific prudential requirements, governance and

operational resilience arrangements and insolvency policies to strengthen the resilience of custodial activity and protect investors.

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.

In DCGG's view, the considerations for potential technological risks arising from crypto-related activity laid out in Chapter 8 provide a sufficient understanding of the sector. Noteworthy, regulators should encourage the deployment of specific audits of the underlying technology and cyber security mechanisms for the purposes of effective oversight and risk mitigation.

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

The deployment of audits of smart contracts, code and technological functionalities are a sound tool for risk assessment and evaluation prior to launching a product. In addition, having in place sound internal control mechanisms with regard to CASPs, as mentioned throughout this paper, can significantly increase the resilience and level of investor protection embedded in the services provided to the end customer. In terms of communicating this information to consumers, we support transparent disclosures in non-technical language (through the crypto-asset whitepaper for tokens and through websites and other relevant information sources for CASPs) to facilitate the investor journey and inform risk tolerance prior to engaging with the product or service.

Chapter 9
Recommendation for Retail Distribution

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

Suitability and appropriateness assessments, as proposed under Chapter 9, are sound safeguards to promote consumer protection. In order for these assessments to provide the highest level of security possible, we encourage cooperation between regulators and the crypto-asset industry to ensure all aspects of the specific implications and particularities of sale and distribution processes. In addition, we recommend the development of disclosure requirements on the risk level of crypto-asset promotions in marketing materials to comprehensively inform investors accessing and operating on a certain CASP.

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

In DCGG's view, promotions are an integral part of engagement with the sector, as long as it is done responsibly and transparently. With this in mind, we disagree that advertisements of compliant products and services should be restricted, however, we believe it would be reasonable for regulators to enforce safeguards for the way such products and services are advertised, namely through disclosures communicated through all the channels and means for promotions on the potential risks involved, similar to what is applied to traditional finance. This way customers would receive all the necessary information at the outset of their investor journey and would be able to make an informed decision aligned with their risk tolerance level.

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.

DCGG and its members understand the IOSCO recommendations and outlined features with regard to stablecoins under Chapter 10. However, in our view, it is crucial for regulators to recognise that the generalisation of the approach to different stablecoins highlighted in the Box Test might be harmful to the industry. Introducing more detailed classification on stablecoins would be more beneficial to inform the future regulatory approach to the industry and make it more effective and future-proof. For stablecoins in particular, it is important to differentiate how these tokens operate, including the overarching business and user model, the mechanisms used, such as whether the reserves system is fractional or not, and inter-ecosystem differentiation in terms of traceability and ability to freeze assets (in cases of criminal transfer risks). Comparing it, for example, to traditional asset management regulation and requirements, there is a difference whether it is addressed to professional investors, such as for hedge funds or alternative investment funds, or retail investors, such as through pension funds or retail asset management. This would therefore require specific considerations and obligations to achieve the desired regulatory outcomes.

We encourage IOSCO members to avoid putting the different types of stablecoins under the same regulatory umbrella. Fiat-denominated, crypto-denominated, and algorithmic stablecoins have divergent reserve and stability mechanisms; subjecting these to the same legislative framework without the necessary differentiation, would be inconsistent with their specific characteristics and risk management procedures. Regulators should also be looking at the white papers of different stablecoin solutions to serve as the base for their recommendations to ensure that they are accurate and relevant. Such an approach would be more constructive and sustainable in the long term. It would equally be more practical and reliable for market participants to utilise the white paper and other disclosures *from the stablecoin issuer* when informing themselves as to whether or not to participate with an such a product, rather than requiring a CASP to be directly responsible for speaking to a stablecoin issuers' reserves, mechanisms, rights of holders and so on. This risks inaccurate and inconsistent information being presented to the market between CASPs in the

secondary market. A more practical approach would be to place requirements for such disclosures with the stablecoin issuer themselves, through mechanisms such as independent assurance reports on reserves.

Finally, policymakers should also consider the potential of fiat-backed stablecoins to enhance financial stability for the crypto assets market. These assets allow for sophisticated market participants engaging in cryptocurrency markets to efficiently shift and rebalance capital across global markets. This helps to improve price discovery, which is the best deterrent to financial instability. Regulations should therefore be flexible enough to take into consideration the purpose of the crypto asset or stablecoin, whether it is likely to achieve mass adoption, and the mechanics of its operation (e.g., the reserves management framework, stability mechanism, how it generates income) - this would ensure the necessary proportionality and fairness for this strand of the sector, and also harness the benefits of these assets for market stability and consumer protection.