Gruppe Deutsche Börse

Comments on IOSCO´s Consultation Report CR01/2023:

„Policy Recommendations for Crypto and Digital Assets Markets"

Frankfurt am Main, 18th July 2023

I. General remarks

Deutsche Boerse Group (DBG) welcomes **IOSCO's on-going efforts to further enhance market stability and market integrity** by adressing related concerns arising from crypto-asset activities.

We welcome **IOSCO's valuable work with regard to DLT/digital assets**, while being outspoken proponents of **high, globally agreed common standards -** especially given the global nature of digital asset and related crypto-activities - that **avoid market fragmentation and ensure market integrity.**

As an operator of several "traditional" trading venues, clearing houses (CCPs) and central securities dopositories (CSDs) **Deutsche Börse Group has a long-standing expierence in building markets** and **implementing several safeguard mechanisms on these markets in best interest of investors**.

Technological innovation – such as Distributed Ledger Technology or Cloud – **enrich the development of future financial markets**. Especially, DLT has the potential to deliver lower costs, faster execution of transactions, improved transparency, auditability of operations, and other benefits.

However, having seen the recent events in the **crypto-assets industry in our view regulation and common standards are a key element** to foster **market integrity and consumer protection.**

It is time to **bring the crypto-asset ecosystem to the same level of regulation as the "traditional" financial system**. **"Same business, same risks, same rules" should apply as a general principle,** while **"tech-neutrality" has to be ensured**, as the lessons learned from the financial crisis 2008/9 are still valid and important, especially if technology changes. Given the lack of expierence and new realities that might bring new (additional) risks which need to be considered.

Therefore, we are in favour of a very close global alignment of regulators and existing regulations. Although we acknowledge the difficulty in finding a right balance between **not "re-inventing the regulatory wheels",** but **also not to just "copy-paste" elements**, but rather **adopt to new circumstances.**

We welcome the opportunity to comment on IOSCO's consultation report "Policy Recommendations for Crypto and Digital Asset Markets" and want to give some answers on the questions below.

II. Comments in detail

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

DBG response: We agree with recommendation 1. Some further comments:

- We welcome the direction of travel that IOSCO sets out in this consultation.
- "Same business, same risks, same rules" should apply as a general principle.
- Technology neutrality must be ensured.
- We support the establishment of rules for crypto-asset service providers (CASPs): in Europe, we have just recently (9th June 2023) seen the publication of the Markets in Crypto-Assets Regulation (MiCA) in the European Official Journal. MiCA institutes uniform EU market rules for crypto-assets. The new legal framework will support market integrity, financial stability and consumer protection by regulating public offers of crypto-assets and by ensuring consumers are better informed about their associated risks.

- The proposed IOSCO recommendations should be aligned as close as possible to the rules MiCA already has foreseen in Europe – one of the largest crypto economies worldwide, as recently referred to in the Chainalysis' geography of cryptocurrency report 2022.
- Not all crypto-assets are the same, and therefore should not be treated in the same way. We would differentiate between digital assets (e.g. DLT issued securities) versus payment assets (like stablecoins or asset-reference tokens or cryptocurrencies). Especially, those digital assets which have as an "underlying" a traditional financial instrument like, shares, bonds etc. should be treated as a financial instrument and fall under already existing regulation/principles.
- We would like to point out that there are already existing frameworks for "traditional" financial infrastructures / assets classes, which need to be adopted to "digital assets" and should take into account the specificities of DLT (e.g. in the EU for example, EMIR was drafted longtime before DLT technology was invented). Therefore, we would recommend, to integrate in an IOSCO classification of digital assets all forms of DLT instruments, including crypto-currencies, DLT securities, DLT derivatives, but also new concepts as for example "Decentralised Finance" and "Staking".
- When proposing recommendations for a new type of assets class such as digital assets the principle of "proportionality" in key.

***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?*

DBG response: DBG advocates the application of existing regulations by incorporating DLT into today's products and services and by adapting interpretation of the provisions to a DLT environment. This would facilitate or even avoid the complete review of certain legislation already established in the financial markets. If needed, new regulation like in the EU the MiCA framework should be developed with principles known in traditional finance like investor protection and ensuring market integrity.

***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?*

DBG response: Conflicts of interest must be avoided. DBG is a supporter of the usual rules as in traditional finance. However, instead of having very strict rules, it's better to have options to solve this problem by governance. In the EU, MiCA already requires rules such as segregation of client assets.

***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?*

DBG response: Conflicts of interest should be addressed in specific licensing requirements. The strict requirement of "separation of legal entities" however, is to be questioned and should only be used as a tool of "last resort" as there might be better ways (e.g. like governance, splitting particular functions, establishing effective conflicts of interest policies, procedures and controls and provide public disclosure and reporting) to resolve conflicts of interest. Having an infinite number of companies is not a solution to allow for innovation, and it is important not to render recommendations/rules too complex. We would like to remind that the existing framework already caters for this type of risk mitigation. Disrupting existing, well-functioning concepts does not add to legal certainty.

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

DBG response: A single group or entity in traditional financial services, CeFi or DeFi providing multiple functions might be a more effective way of delivering services. Exchange groups in TradFi often expand their business portfolios to diversify their revenue streams and create synergies among their various subsidiaries. This diversification helps mitigating risks and stabilise financial performance thereby helping to deliver financial stability. For example, an exchange group that owns a stock exchange and a CCP can leverage the strengths of each business to enhance efficiency and competitiveness.

Moreover, owning multiple businesses can provide economies of scale, allowing exchange groups to achieve cost efficiencies. Shared infrastructure, resources, and expertise can be utilised across different entities within the group, resulting in reduced costs and increased operational effectiveness. These savings can be passed on to users/consumers to deliver a product at a more competitive price.

Nevertheless, exchange groups have also due to various financial market regulations robust conflict of interest management procedures to ensure ethical and fair practices. This involves implementing policies and mechanisms that prevent any undue advantage or bias among the businesses owned by the group. Transparent governance structures, independent oversight, disclosure requirements, and compliance frameworks are some of the measures that have been proven to mitigate conflicts of interest effectively.

Furthermore, exchanges and other trading venues do not trade against their own clients as a protection against abuses. IOSCO's recommendations should address this situation with regards to CASPs, following the logic that IOSCO is seeking 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."

Disclosure requirements will provide more transparency on the different services provided. It may also be useful to require an ongoing/yearly review of the disclosures made to the public and regulators in all jurisdictions where the CASP operates, and into which it provides services.

In this way, prospective clients, the public and regulators are aware of the new services or possible conflicts of interest that may arise considering the number of differing services being offered by combined CASPs. Just as a reference, for market operator this is already segregated from brokers/market makers (different legal entities, management teams, etc…). Combined CASPs should catch-up with these provisions.

***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?*

DBG response: DBG agrees to strict disclosures when necessary and helpful. Standards should be set as in MiCA, in particular with regard to transparency and liability. The obligation of best execution should apply, as it is designed to promote market efficiency with similar rules for similar outcomes.

***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.*

DBG response: Under MiFID, there is a prohibition for MTFs, which means that it is not allowed to execute orders against the own books. Brokers and custodians should not co-mingle. Crypto-asset exchanges, like traditional exchanges or MTFs should be ideally set-up as "neutral" infrastructure. On the one hand, there must be clear rules that prevent conflicts of interest, but complete separation of legal entities seems not beneficial in all cases.

Subject to proper oversight, any combination of services within a legal entity should be possible, as in traditional financial markets, unless there is a specific reason not to combine certain functions. If the conflict is regulated in another way, you do not need a separate legal entity.

As is traditional finance the services of MTFs should be separated from broker/market maker services, thus combined CASPs need to segregate their "exchange" entities from other service offerings in order to be a neutral infrastructure.

In the pursuit of 'same risk, same regulation' it is worth considering how things work in TradFi. Regulatory bodies often impose strict rules and safeguards on firms operating trading venues while also acting as trading intermediaries. These may include robust conflict of interest management, surveillance systems to detect market abuse, transparency requirements, and the establishment of independent oversight committees or regulatory bodies to ensure fair and transparent operations Therefore, at the very least, IOSCO should seek to apply the same strict rules and safeguards on firms operating trading venues while also acting as trading intermediaries.

"Prohibition" should only be possible, but a tool of last resort for conflicts of interests, which are not possible to mitigate otherwise.

IOSCO and local regulators could consider strong conflicts of interest policies which could mitigate some of the risks.

***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?*

DBG response: DBG supports "standard" reporting, equal to MiFID with some "reliefs for crypto-assets" to take the "proportionality" principle into account. Conducting transactions "off-chain" can offer significant benefits. The trading and settlement platforms can benefit from costs-savings related to gas fees as well as increased internal efficiencies. However, IOSCO rightly notes that there is a risk of a loss of transparency in the market.

Therefore, CASPs could be required to report in similar ways to exchanges and alternative venues in TradFi. For example, post-trade rules generally require the price, volume and time of transactions executed on the trading venue.

***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?*

DBG response: MiCA is a good role model to start, because it mandates whitepapers with adequate information disclosure to prevent knowledge asymmetry among market participants. However, as not everything fits into the crypto realm, it is not possible to reproduce everything from "traditional" finance to it. Scams need to be prevented.

***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.*

DBG response: We welcome the proposed recommendations on listings. Minimum requirements for listings will help to build trust in these products.

***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 behaviours and enhance integrity?
b) Any novel offences, or behaviours, specific to crypto-assets that are not present in traditional financial markets? If so, please explain.

DBG response: No response

***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*

DBG response: Technological tools addressing the identified risks of market abuse are available.

***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?*

DBG response: To foster cooperation, DBG proposes close coordination in international forums and among existing industry experts and committees. Harmonisation and reliance on mutual standards would be effective in supporting cross-border co-operation and managing cross-border trade.

When regulatory frameworks are harmonised, regulatory authorities can have a common understanding of the requirements and expectations for market participants. This consistency simplifies cross-border transactions and enhances cooperation by reducing regulatory complexity and confusion.

Moreover, when standards and regulations are aligned, it becomes easier to exchange information and communicate effectively. Regulatory authorities can collaborate on areas such as risk assessment, supervisory practices, and enforcement actions, enabling to make better-informed decisions and coordinate efforts and reducing the possibilities for regulatory arbitrage across borders.

In situations where financial institutions or market infrastructures operate across multiple jurisdictions, harmonised regulations facilitate coordinated supervision, risk assessment, and crisis response. This cooperation helps prevent regulatory gaps, promotes stability, and ensures a more coordinated approach to addressing potential risks and crises.

This initiative by IOSCO is an excellent starting point for harmonisation and co-operation. However, without mutually agreeing definitions for crypto-assets it will be difficult to encourage co-operation.

***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?*

DBG response: We would like to refer to MiCA as a benchmark, which defines minimum requirements and has rules for CASPs. It already contains very heavy obligations of custodians such as being 100% liable for client losses due to cyber-attacks. Thus, it is preferable that other regulatory regimes also apply at last the same level, otherwise there's a chance for regulatory arbitrage between markets.

***Question 15**: – (a) Should the Recommendations in Chapter 7 address the manner in which the customer crypto-assets should be held?*
(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?
(c) 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?
(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.

DBG response: In any custody arrangement for digital assets, the security of the private key holds high importance. Critical decisions must be made regarding the storage format, environment, and the procedures and timelines involved in utilising the private key for transaction authentication. In general, there are three options for storing the key:

(a) "self-custody" or a "non-custodial" arrangement, where the client retains control over the key
(b) a "custodial" arrangement, where a custodian securely stores the key on behalf of the client; or
(c) a hybrid of the two.

The wide array of available services and solutions in the market has a direct impact on the legal ownership and risk assessment that clients must undertake. It is important to recognise that these analyses will vary in each case, as there is no universally applicable approach.

Solutions that provide clients with the private key, known as self-custody or non-custodial wallet solutions, may not fulfil the rigorous financial crime protection, security, and deployment requirements of sophisticated institutional clients in the present landscape. Moreover, these self-custody solutions may be inappropriate for unsophisticated investors.

Further, one could differentiate between a "private investor", who should be allowed to go any of the three custody options and an "institutional investor", such as asset management who act as fiduciary for the clients. For these, self-custody is only an option, in case they have sufficient capabilities to do so, otherwise outsource to a specialised CASP-Custodian would be a better way.

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

DBG response: DBG refers to MiCA, when it comes to prudential requirements. At the same time, we point out that it is necessary to consider that technological risks for crypto-assets are much higher.

Alongside the task of protecting digital assets, digital asset custodians bear the responsibility of maintaining intricate and demanding security measures. These custodians have experienced a recent surge in hacking incidents, leading to the theft of customers' digital asset wallets in numerous instances. While cybersecurity risk is not a novel concept, the methods employed by hackers to gain unauthorized access and exploit assets/funds have evolved along with technological advancements.

In such situations, customers rely on the terms set forth by the digital asset custodian and, to a certain extent, the custodian's willingness to compensate for the stolen assets. For example, MiCA states clearly the custodian will be liable for the client loss due to “incidents that are attributable to them”.

***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.*

DBG response: We agree with the recommendations. However, we would like to refer to the DORA regulation in the European Union, which aims to create a uniform framework for managing cybersecurity risks in financial markets. DORA addresses already CASPs. We also see similar recommendation from IOSCO in these areas.

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

DBG response: Retail clients should only be served by licensed companies in their jurisdictions. This is important to protect especially retail investors. Guidance on “Reverse solicitation” is a topic on how to address/minimize opportunities for unlicensed players accessing regulated jurisdictions.

There are unique technology/cyber/operational risks related to crypto-assets but they are principally linked to the type of DLT being used, rather than the use of DLT per se.

For private DLT (like tokenised traditional securities), the risks are substantially the same. This is because the DLT is controlled by a single entity that can fix errors in the system. For public DLT (like Bitcoin and Ethereum) no one entity can step in and fix errors in the system.

Public DLT remains at risk of attacks like these or even more simple hacks where the fund movements are hardly reversible or even irreversible. Therefore, it is important for CASPs which serve retail investors directly to undertake proper risk assessments of the DLT that they enable trading of and to disclose these risks in a clear, digestible format.

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

DBG response: Currently, regulated retail brokers are reluctant to start offering crypto-assets to their private investor base mainly due to unclear regulation about what needs to be disclosed to private investors. This clarity is of utmost importance to provide retail investors a regulated channel for their transactions in crypto-assets.

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

DBG response: The rules of each jurisdiction should also be applied to companies from third-countries being active in these jurisdiction to avoid regulatory arbitrage.

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

DBG response: In the EU, MiCA already applies, but clearing of stable coins should be included.

***Question 22**: – IOSCO also welcomes views from stakeholders on potential additional issues for consideration*

DBG response: DBG supports the inclusion of clearing and NFTs, as they are not yet covered.