Response of Deutsche Börse Group on IOSCO's Policy Recommendations for Decentralized Finance (DeFi) Consultation Report

Frankfurt am Main, 18th October 2023

Introductory remarks

Deutsche Börse Group (DBG) in its capacity as a financial market infrastructure provider uses modern IT and other technological solutions to operate and service the financial sector worldwide. Technology is at the core of our operations and is an integral part of the regulated services we operate. We ensure the efficient functioning of markets, including but not limited to market data, trading, provision of indices, clearing, securities custody.

DBG clearly sees the advantages of new technologies and is actively seeking to use them. We are familiar with the handling of financial market instruments and different asset classes since decades, and we understand very well the risks associated with new types of crypto-assets.

We are currently working on the use of cloud technology and Distributed Ledger Technology (DLT)/blockchain as well as on the further automation of processes. We use these technologies in a tested manner, hence continuing to guarantee transparency, stability and investor protection at all times.

In this context we acknowledge the IOSCO's valuable work at monitoring developments in crypto-assets, trading and settlement on DLT andd its published principles on Decentralized Finance.

Deutsche Börse Group responses to selected IOSCO questions

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

Deutsche Börse Group supports the proposed nine policy recommendations by IOSCO. However, we would like to highlight the following aspects:

We see the trend of Decentralised Finance (DeFi) emerging with financial products built on DLT networks, often on public blockchains. These pure peer-to-peer layers offer their financial services to (retail-) clients without a central intermediary implying certain rules automatically on the basis of e.g., programmed Smart Contracts. Although they might bring innovation to financial products, the concept is new and attracting growing interest recently.

It will be important to protect consumers/investors the same way, as if they would buy "traditional" financial services. FMIs could fulfill such important functions/roles, as not every task could be "outsourced" to the technology only.

We share IOSCO's view that a regulator should achieve a holistic and comprehensive understanding of DeFi products, services, arrangements, and activities. Therefore, we support that the international DeFi regulatory framework should maintain a technology-neutral approach.

We further concur with the report's evaluation that the notion of "decentralisation" in Decentralised Finance (DeFi) services can often be more illusory than real. Many of these services essentially mimic traditional financial mechanisms – but with less oversight and greater risks to investors.

Going forward, in our view it is important to combine the best of both worlds DeFi and Traditional Finance (TradFi), combining the trust and scalability of traditional financial markets with openness and integration between legacy systems and the digital world. We are going to be guided by the

need to rethink business models, introduce new paradigms and ways of thinking, but not overhaul but find a smooth transition from old to new. It is of utmost importance to uphold the values of transparency, fairness, stability, investor protection, and market integrity.

The first crucial step towards regulating them is to accurately categorise the different products and services within the digital space. We note, in particular, that the label 'decentralised exchange' may suggest something it is not. It might give the impression that the platform is without centralised control – an assumption IOSCO mentions as not necessarily true. It might also give the impression that it is regulated and can be trusted to have certain controls in place like a traditional exchange. The risk arising from this misleading terminology is evident: retail investors can be, and often are, misled by the terminology.

In addition, regulators should ensure that the DeFi framework is aligned with existing regulations (e.g., the MiCA Regulation in the European Union). Redundant regulations should be avoided, and there should be a tailor-made regulation that is adapted to DeFi specific characteristics and risks. Furthermore, future DeFi financial regulation requires an understanding of the entirety of the DeFi system and its interrelation with CeFi, TradFi, and other actors in this space, as outlined in the guidance section of Recommendation 1.

Recommendation 2 – Identify Responsible Persons

We welcome the report's focus on identifying responsible persons and holding them to account, much like a regulator of traditional financial services would.

As IOSCO notes, decentralized entities often act automatically but they do not arise out of nothing. The decentralized entities are created, developed, and governed by groups of people. The persons that exercise control or sufficient influence over a DeFi arrangement or activity should be identified in order to see if they meet standard regulatory requirements of trusty competence, capability, and financial soundness. Holding controlling persons of DeFi applications and protocols accountable is a crucial aspect of delivering technology-neutral regulation in the rapidly evolving world of decentralised finance.

We agree that the functioning of the DeFi system sparks numerous questions as to formal legal accountability in cases of fraud and mismanagement of the system.

Given that transactions take place in a cross-border scenario, it is not clear which jurisdiction would apply in cases of violation. Considering that anyone can participate in the trading in an anonymised manner, it is difficult to establish which party to hold to account in cases of fraud.

Regulators should also consider different monitoring procedures in order to ensure that all market participants involved in transactions are held accountable in case of misconduct, fraud, market manipulation, etc. Such monitoring could be ensured by introducing KYC/AML requirements at client level.

Where Smart Contracts are coded by numerous programmers or even an "open source", it potentially allows anyone to change its content. Accordingly, DeFi functioning raises questions of who is liable in cases of mismanagement of the system and of how to ensure there is a legal recourse to bring the responsible parties to account. We agree further that it is crucial for Smart Contracts to have identified "owner(s)" or "operator(s)" who will be responsible for their management.

Recommendation 3 – Achieve Common Standards of Regulatory Outcomes

DeFi can serve as an alternative avenue for financial services but also presents many of the same hazards found in the conventional financial sector. Therefore, we welcome the policy goal of achieving the same regulatory outcomes as those that are required in traditional financial markets. In particular, we welcome IOSCO's exercise mapping out the activities and services in DeFi in comparison to TradFi.

In principle, achieving similar regulatory outcomes for DeFi and CeFi (centralised finance) activities, focusing on consumer and investor protection, combating illicit finance, and preserving market integrity, is essential. However, it's also important, as with all regulation, to strike a balance to avoid stifling innovation and fostering regulatory arbitrage.

Recognising that DeFi operates differently from CeFi is also pivotal; effective risk mitigation measures depend on understanding the unique technology and its evolution to manage specific risks effectively. Regardless, the key point here is that the model utilised does not automatically extinguish the risks or obligations for good governance and controls.

Recommendation 4 – Require Identification and Addressing of Conflicts of Interest

We very much agree with IOSCO's attempts to address conflicts of interest in the DeFi world. As we have seen in the CeFi world, traditional failings with regards to conflicts of interest management can and have caused widespread investor harm.

One practice that exchange groups generally avoid is proprietary trading against their clients. This is a frequent occurrence in crypto markets and was a notable issue during the FTX crisis. We believe that there's no viable way to appropriately manage the conflicts of interest that emerge from such activities. Moreover, we argue that any trading platform engaged in these practices should not be entitled to label itself as an 'exchange.

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

We agree that enterprise risk management needs to be taken seriously in the DeFi world. As we have seen in the CeFi world, traditional failings can and have caused widespread investor harm. We generally agree with the assessment and applaud the decision to carefully scrutinise risks attendant to DeFi before prescribing a regulatory framework.

Underlying the question of regulating DeFi is the distinction between the investment and the technology sides of the crypto assets. The investment side looks very much like traditional finance. The technology side, on the other hand, is trying to make these global, permissionless distributed ledger systems actually useful for a variety of activities. This side looks very different from traditional finance, as its functioning is determined by cutting edge computer programming and network building. It is the technology side that introduces novel risks which we should thoroughly understand before we apply regulations. In some instances, it is the technology itself that must evolve to address certain consumer protection, security, and other issues. For instance, regulators must introduce minimum standards for quality assurance of key components within DeFi platforms such as price oracles and data feed sources in general, since the well-functioning of these

components is vital for the reliability and accuracy of DeFi infrastructures. Business continuity and contingency plans should also be in place for critical DeFi components such as oracles.

Therefore, we would caution that the use of public permissionless blockchains/DLTs is being restricted. It is comparable to the internet which is also open and publicly available but depends on the applications/services offered based on it. The same is true for public blockchains – TradFi companies may use the public DLTs just as they use the internet as they bring innovation; it is more important to ensure that the services offered based on it are safe and serve the investors. With regard to appropriate supervision, there are technological tools available in the market which would allow for controlling public permissionless blockchains.

Recommendation 6 – Require Clear, Accurate and Comprehensive Disclosures

We agree with the need for clear, accurate and comprehensive disclosures. Much like exchanges in traditional finance vet products and are subject to rules which enforce disclosures, 'DeFi exchanges' could implement similar measures.

For instance, regulators should define minimum standards and guidelines for asset listing and delisting to ensure that tradeable assets are subject to a verifiable vetting process and meet minimum liquidity requirements in order to prevent market manipulation.

Recommendation 7 – Enforce Applicable Laws

We support the enforcement of applicable laws. Trust is fundamental to the functioning of a markets-based system, and enforcement of applicable laws help foster trust in the system.

Recommendation 8 – Promote Cross-Border Cooperation and Information Sharing

We support cross-border co-operation by regulators.

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

We agree that IOSCO and regulators should further consider the interconnections between DeFi and CeFi as well as to TradFi, as we understand that they might become more interconnected in future. But currently we believe that traditional markets to some degree are isolated from crypto markets through this may change in future.

With regard to custody: As IOSCO notes, several of the market intermediaries in the DeFi space could be undertaking custody activities. Without proper regulation or at least standards, there is a risk that end users could lose their assets.

Finally, we would note that investor education remains of paramount importance. IOSCO has been a global leader in pushing for further investor education – and it should continue to do so more broadly but also in particular for these markets. As IOSCO notes, the extent of decentralization is often not clear and we fear that retail investors could be misled by the term.

Q2. Do you agree with the description of DeFi products, services, arrangements, and activities described in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details.

IOSCO effectively delineates the products, services, arrangements, and activities associated with DeFi entities. This undertaking presents a considerable challenge, owing to existing data gaps and the absence of a universally accepted definition of DeFi. Moreover, ascertaining whether an entity qualifies as DeFi is rarely a straightforward binary determination. Additionally, the term 'de-centralised' introduces confusion, as a central platform facilitating interactions between buyers and sellers can fall within the realms of TradFi, CeFi, or Decentralized Finance.

Notwithstanding, IOSCO's description of DeFi as "financial products, services, arrangements, and activities that leverage distributed ledger or blockchain technologies (DLT), including self-executing code referred to as smart contracts," appears to be excessively broad and susceptible to varying interpretations. It could arguably encompass entities that do not truly conform to the DeFi paradigm. We acknowledge the inherent complexity in achieving a consensus on the definition of DeFi among 238 members. Nevertheless, we propose that establishing guiding principles or offering clarifications, particularly concerning the absence of centralisation and/or intermediaries, may yield valuable benefits.

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

It is imperative that decentralised governance within the DeFi space adheres to best practices and standards with regard to governance mechanisms. This is essential not only for investor protection but also for establishing and sustaining trust in the entire blockchain ecosystem.

Q4. Do you agree with the risks and issues around DeFi protocols identified in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants help address these risks and/or issues, including through the use of technology? How would you suggest IOSCO members address these risks and/or issues?

We agree with the risks and issues outlined in the report, in particular with those stemming from the issue of identification of responsible parties.

One significant weak point in the DeFi landscape is the risk associated with Smart Contracts. Smart Contracts are also often coded by numerous programmers or even an "open source" that potentially allows anyone to change its content. Accordingly, DeFi functioning raises questions of who is liable in cases of mismanagement of the system and how to ensure that there is a legal recourse to bring the responsible parties to account. If these contracts are not thoroughly audited, tested, or secured, they may harbour flaws that could be exploited by malicious actors. Should such an attack happen, it could lead to the loss of assets stored in the affected contract.

Moreover, if a hacking or exploitation event takes place, the digital assets stored in the Smart Contracts or on the 'decentralised exchange' (DEX) could be misappropriated, resulting in heavy losses for asset owners. Additionally, if the DeFi ecosystem were to face a liquidity crunch, it could erode the value of crypto assets, subsequently affecting the overall worth of portfolios managed by custodians.

There are also significant risks of money laundering and terrorist financing as many DeFi products and services do not have requirements to abide by AML/CFT rules. Additionally, there is always a risk that a traded coin is "tainted" as it could come from a wallet that is connected to illicit activities. In current market practices, firms decide based on their own assessment how much risk they are willing to take, as any coin could become tainted. Therefore, companies need to develop risk assessment methods when deciding on how to proceed with such tainted coins. Additionally, the whole industry would benefit from industry-wide standards and guidance.

Due to its decentralised nature and complexity, the regulation of DeFi is a challenging task that requires careful consideration.

We support that regulators take the time to understand the developments and assess them at a later stage, and if so, how to regulate DeFi. CeFi institutions, however, should be allowed to enable easy, reliable, and efficient access (on and off ramping) to DeFi applications. They would act as trustworthy intermediaries and build a regulated bridge between CeFi and DeFi. It is important not to "overburden" the requirements for regulated players to enter and test the new space by trying to adapt to the same safeguards known from traditional asset classes.

Meanwhile, one could try to facilitate the interactions between regulated players and DEXs. One way to do this could be to allow regulated Financial Market Infrastructures (FMIs – such as regulated markets, multilateral trading facilities, CCPs, CSDs) to interact with DEXs, after validating the "minimum" technical standards of a Smart Contract in question and involving independent technical auditors.

Additionally, since CeFi institutions are able to comply with regulatory standards by fulfilling AML criteria, CFT, and KYC, and ensuring investor protection, they can provide users with security and reliability in using DeFi applications.

Q6. Do you agree with the application of IOSCO Standards to DeFi activities contained in this Report? Are there other examples of how IOSCO Standards can apply?

Yes, we support the applying of the IOSCO standards to DeFi activities to make it consistent with the goal of achieving the same regulatory outcomes for DeFi as there is in TradFi.

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

Regulation of real DEXs will prove to be a difficult task for regulators and policymakers: whether to regulate at the protocol level or the application level and finding the liable entity who is responsible for the protocols, Smart Contracts, and the applications.

One of the possible regulatory approaches could be to regulate the issuance and management of Smart Contracts. However, it would be a challenging task as supervisors will need to control the technology used ("Smart Contract Audits") and the coding skills of programmers – which would be a completely new/different kind of supervisory mechanism/approach.

It is finally crucial to keep the balance between innovation and safety for financial markets. From an operational perspective, a potential approach should be more detailed, but we avoid recommending technology-specific parameters. For example, including the disclosure of material

information similar to those applicable to TradFi on products, services, and underlying entities would be a very good way forward.

Additionally, the regulatory approach should focus more on transparency for and education of users of potential risks stemming from DeFi rather than restriction of their participation in DEXs trading.

Q8. Given the importance of the application of IOSCO Standards to DeFi activities, are there technological innovations that allow regulators to support innovation in DeFi/blockchain technologies while at the same time addressing investor protection and market integrity risks? If so, please provide details.

As the technology space is developing, there will be some interaction between traditional trading and the use of DEXs.

Therefore, we would caution that the use of public permissionless blockchains/DLTs is being restricted. It is comparable to the internet which is also open and publicly available but depends on the applications/services offered based on it. The same is true for public blockchains – TradFi companies may use the public DLTs just as they use the internet as they bring innovation; it is more important to ensure that the services offered based on it are safe and serve the investors.

In situations where fully-fledged decentralised exchanges are not suitable, there is still a possibility to introduce certain DEX-specific mechanisms to traditional exchanges. They would benefit from new blockchain-based efficiencies while maintaining regulatory certainty.

Q9. Are there particular methods or mechanisms that regulators can use in evaluating DeFi products, services, arrangements, and activities, and other persons and entities involved with DeFi? If yes, please explain.

As mentioned earlier, regulated CeFi/TradFi institutions could provide an array of safeguards and reliability to the world of DeFi. In this regard, activities of CeFi/TradFi institutions in enhancing the decentralized networks' integrity, e.g., by contributing to the consensus mechanisms or by running nodes for the networks, should be encouraged and be allowed. It is worth mentioning that consensus mechanisms are not DeFi products or services and, thus, are free from some of the risks of other financial activities (e.g., counterparty risks). Furthermore, protocol mechanisms are the necessary foundation for blockchains' integrity on which DeFi products and services are built. Hence, the industry should foster this nascent array of services, policymakers should regulate them, and CeFi/TradFi institutions should contribute to upholding their integrity.

***

We hope that our comments will be helpful, and we stand available for any clarifications and further discussions.