Registro das Reflexões sobre as Questões da Consulta IOSCO *"Policy Recommendations for Crypto and Digital Asset Markets Consultation Report"*

Laboratório de Inovação Financeira

GT Fintech

Subgrupo de Inovação e Soluções de Mercado

14 de julho de 2023

Introdução

Buscando atender a uma solicitação da Comissão de Valores Mobiliários (CVM), o Subgrupo de Inovações e Soluções de Mercado do Grupo de Trabalho Fintech (GT Fintech) do Laboratório de Inovações Financeiras (Lab) realizou durante parte dos meses de junho e julho um debate sobre os principais pontos trazidos pela consulta pública da IOSCO "*Policy Recommendations for Crypto and Digital Asset Markets Consultation Report*"[1], publicada em 23.05.2023. A realização desta discussão teve como objetivo contribuir com a análise e resposta que a Autarquia enviará à entidade internacional, no sentido de trazer reflexões sobre os pontos tratados pela consulta, para que possam servir de insumo para a CVM, no que couber e julgar pertinente . Desta forma, segue abaixo o registro das principais considerações debatidas pelos os membros do Subgrupo de Inovação e Soluções de Mercado sobre o tema em questão. Trata-se de um documento interno do LAB que está sendo elaborado em apoio à CVM.

Em termos de organização das discussões, caso seja útil à Autarquia, a gravação de todas estas reuniões foram reunidas em um drive compartilhado com a CVM (disponível aqui). Ademais, elencamos abaixo as datas das reuniões realizadas e respectivos pontos da consulta IOSCO debatidos:

- 1º reunião (realizada em 20.06.2023 de 11h às 12h30):
  - 1 - Overarching Recommendation Addressed to All
  - 2 - Recommendations on Governance and Disclosure of Conflicts
- 2º reunião (realizada em 26.06.2023 de 10h às 12h)
  - 3 - Recommendations on Order Handling and Trade Disclosures (Trading Intermediaries vs Market Operators)
  - 4 - Recommendations in Relation to Listing of Crypto-Assets and Certain Primary Market Activities
- 3º reunião (realizada em 03.07.2023 de 10h às 12h)
  - 5 - Recommendations to Address Abusive Behaviors
  - 6 - Recommendation on Cross-Border Cooperation
  - 7- Recommendations on Custody of Client Monies and Assets
- 4º reunião (realizada em 10.07.2023 de 10h às 12h)
  - 7- Recommendations on Custody of Client Monies and Assets (*Continuação*)
  - 8 - Recommendation to Address Operational and Technological Risks
  - 9 - Recommendation for Retail Distribution
- 5º reunião (realizada em 11.07.2023 de 15h30 às 17h30) - revisão final

O Subgrupo de Inovação e Soluções de Mercado do GT Fintech LAB agradece a oportunidade de contribuir com a reflexão sobre os temas destacados na consulta IOSCO e coloca-se à disposição da CVM para novas contribuições.

[1] Consulta IOSCO disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf

Reflexões sobre a Consulta IOSCO

O registro dos debates está organizado de acordo com os principais capítulos da consulta (capítulos 1 a 9) e busca responder às suas respectivas perguntas. Com relação às questões adicionais da consulta, trazidas em seu capítulo 10 ("Chapter 10: Box text on Stablecoins"), devido ao prazo mais exíguo das discussões, comentários foram facultados aos membros para envio por e-mail - contudo não recebemos considerações. Adicionalmente, ao final deste documento, buscamos também registrar reflexões auxiliares aos debates em um anexo. Ali registramos uma tentativa de sistematizar possibilidades assumidas pelos tokens (o que o grupo denominou de "árvore de decisões de tokens") que possam ser úteis para identificar situações com maior ou menor risco, as quais devem ou não suscitar maior atenção dos reguladores. Trata-se de um esforço inicial e não exaustivo de sistematização e que traz questões ainda em aberto, mas que buscamos também disponibilizar aqui para subsidiar as considerações feitas.

Seguem as principais considerações do subgrupo a respeito da consulta:

General remark:

Regarding the scope of the considerations, some participants called attention to the fact that they believed they should seek to place their considerations mostly on securities, since the consultation is intended to support the Brazilian Securities Commission's reply to IOSCO. Other participants mentioned that IOSCO seemed to be requesting opinions of its members also in relation to "grey zone" assets, which should include non-traditional forms of investments and maybe even assets that are not firmly established as securities, such as BTC, ETH and other protocol tokens. Also, the emphasis in CASPs given by IOSCO may bring about such discussion. Therefore, whenever possible, more general considerations, in addition to securities, will be made to record the discussions made in this document.

1 - OVERARCHING RECOMMENDATION ADDRESSED TO ALL

Recommendation 1 – Common Standards of Regulatory Outcomes

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

There is consensus among participants around the idea that the recommended measures are important for investors protection, especially retail investors, as well as for the integrity of the crypto asset market. However, given the innovative characteristics of this market there are different perspectives on how regulation should deal with it. On the one hand, using existing rules, even if the innovation requires, implicate in some modernization; on the other hand, to create specific new regulations for crypto assets, one designed with special attention to the characteristics of this market.

Part of the group understands that **existing regulatory frameworks could be extended and adapted** for activities related to crypto assets. The importance of a "friendly" posture by the regulator in relation to the development of new technologies is reinforced, but the aim is to maintain a posture of the regulator as neutral from the point of view of which technology will be used. The idea is defended that the regulator maintains investor protection and market integrity, while opening space for the development of new markets or more efficient ways of performing services and activities. However, without generating new and higher compliance costs. There is, therefore, a doubt here whether specific adaptations in the existing regulation could generate some kind of regulatory arbitrariness between crypto markets and traditional markets.

Additionally, some participants also mentioned the need to **include "innovation" as a principle and objective** of the regulatory framework for digital assets. This suggestion is related to the mandate Brazilian regulators (and other regulators around the world) received from legislators[2] of promoting innovation and technology in capital markets.[3] As argued by the participants, the regulation of digital assets may require waivers and special authorizations, as well as regulatory sandboxes and room for experimentation.

[2] Under the Brazilian Securities Commission Act (Law # 6,385/76, art. 4, I and III), the Brazilian Securities Commission is tasked with the mission of developing capital markets, amongst others such as protection of investors (art. 4, IV and V) and promoting the efficient and well-functioning capital markets (art. 4, III, VII and VIII). This mandate allowed the Commission to pursue innovative approaches to regulation such as the creation of crowdfunding platforms, the regulatory sandbox regime, new security instruments such as the "Agro" funds, and the authorization of investments funds in crypto assets. See also the confirmation hearings of Commissioners Otto Eduardo Fonseca de Albuquerque Lobo and João Pedro Barroso do Nascimento.

[3] The SEC also includes amongst its core missions the promotion of innovation in capital markets. The Goal 2 of its mission statement includes "Develop and implement a robust regulatory framework that keeps pace with evolving markets, business models, and technologies". See https://www.sec.gov/our-goals.

Participants also mentioned concerns with **"fragmentation" and unleveled playfields**, which could bring about dual regimes of regulation for digital and analogic assets. Concerns also related to favoring centralized business models in detriment to more neutral approaches, and the need to level the playfield in order to allow for the development of digital asset markets, and avoid digital assets to be treated as assets different from their analogic versions. Many regulatory regimes trust in centralized infrastructures to control access to markets and give special powers to gatekeepers, which may hinder the adoption of decentralized technologies and protocols, and push digitalization to niches. Digital assets should not be considered alternative markets, and the digital and analogic versions of the same assets should be deemed as having the same nature, thus be subject to similar regulatory standards.

Another part of the group's participants defends the idea of a **new regulatory framework** because the current regulation would not be the most suitable for activities related to actions and structures linked to crypto and digital assets. Cryptoassets have their own characteristics of disintermediation and role changes that could lack a more customized framework. According to these members, in the short term, it would be possible to make some waivers in existing regulations to accommodate new innovation structures. However, in the long term, as the markets progress, a greater change in regulation seems to be necessary, which some of the members even pointed to as a new regulation. For them, regulation today is based on roles and responsibilities, attributions, to certain actors and agents (such as gatekeepers of certain functions). However, the structure of crypto assets allows the different activities to be performed by other and different actors. For example, activities of a tokenizer include bookkeeping and distribution responsibilities. Or the exchange takes over custody, trading and settlement activities. That is, for part of the members, for these changes in the arrangements of roles and responsibilities to occur, preserving the necessary principles and safeguards of each activity, a major change in regulation would end up being necessary, which they understand as even a new regulation.

2 - RECOMMENDATIONS ON GOVERNANCE AND DISCLOSURE OF CONFLICTS

Recommendation 2 – Organizational Governance
Recommendation 3 – Disclosure of Role, Capacity and Trading 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?**

The group agrees that there are different conflicts of interest generated mainly by the possibility of aggregating different activities under a "same roof" in the CASP's activities. Consequently, it supports that these conflicts should be mitigated and avoided using different strategies.

Although it is not possible to exhaustively predict all possible conflicts that may occur in CASP's activities, the group points out that, as some conflicts already have been identified and mitigated by traditional

regulation. The traditional framework could be useful to identify CASP's conflicts. Additionally, in general, what happens is that in the crypto market, **new actors or new access permissions and functions emerge that can reactivate risks already mapped and mitigated by traditional systems**. Following are examples of some conflicts that may become more feasible and frequent, still persist in the crypto world, and that had already been controlled by traditional regulation (also mapped by the IOSCO consultation itself): (i) prop trade vs privileged information regarding order flows; (ii) asset lending vs key custody - appropriation of client assets; (iii) CASP business models in which they are both distributor (intermediary) and market; (iv) conflict between role of distributor (brokerage) and organized market; (v) supplemental listing conflict where exchanges place greater emphasis, information and promotion on tokens in which they have a stake.

- **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?**

The group agrees that conflicts of interest should be addressed. However, they diverge regarding the need or not for certain segregations and prohibitions to address these conflicts.

Some of the members argue that some conflicts of interest should be treated in the same way as traditional markets. Some cases require certain **prohibitions and segregations**, for example, the case of intermediaries and market operators. It is even a form of treatment to avoid regulatory asymmetries in crypto markets and traditional markets.

In other ways, some of the participants disagree that this is the best way to deal with CASP activities. They point out that, unlike the traditional regulation, **in some cases different activities and services may be allowed under the "same roof" in a CASP, but disclosure mechanisms and strong supervision must be strengthened**. It was argued that there is a great dispersion of entities operating in the crypto market. In general, they are smaller entities that act by aggregating different activities under the "same roof", which guarantees them economic efficiency gains. A possible solution would be **requirements for segregation of activities proportional to the size of CASPs and their risks**.

As previously mentioned, some examples are exchanges that operate in custody, trading and settlement activities. Separating these activities and demanding the same traditional regulatory requirements from them could make many of the smaller companies currently active unfeasible, whose business is made possible by gains in scale, scope and efficiency. For these participants, the separation of activities or prohibitions could avoid certain conflicts and bring security, but could also generate the closure of the activities of certain smaller CASPs. An alternative could occur through some exemptions from segregation in the case of smaller companies, but with the counterpart of certifying its procedures and segregations and giving disclaimer about its measures to avoid conflicts of interest.

Additionally, these exceptions could no longer be applied in cases of large CASPs, which operate certain high levels of asset volumes, and which start to generate systemic risks. For these cases, traditional segregations and prohibitions could be applied. In other words, structuring rules that are stronger and proportionate to the volumes transacted and the risks involved. The members therefore suggest, in this way, regulation could be more sensitive to the current economic business models of crypto markets - which do not make smaller CASPs unfeasible, but adopt security measures against conflicts proportional to the

risks observed in big CASPs.

Still on the separation of activities and which activities the CASPs should undertake, the participants highlighted the possibility of **separating key custody (custody) from distribution and trade**. For example, CASP should establish mechanisms of controls and internal governance for this separation, keep information available to certify these separations and provide due disclosure. Or it could even be the case of formal separations into larger CASPs, proportionally to the volumes of assets and risks presented.

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

Regarding auxiliary ways to address conflicts of interest of CASPs and its disclosure, the group reinforces the path of **self-regulation**. This could help implement the regulation, handle more routine details and operational specifications. In these cases, self-regulation could address structure good practices, details of disclosure standards and support supervisory processes for these potential conflicts.

3 - RECOMMENDATIONS ON ORDER HANDLING AND TRADE DISCLOSURES (TRADING INTERMEDIARIES VS MARKET OPERATORS)

Recommendation 4 – Order Handling
Recommendation 5 – 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?***

Participants agree with Recommendations 4 and 5 and understand that they will have a positive impact by giving CASPs operating as trading intermediaries a greater responsibility to act in the best interest of their clients and seek the best conditions for executing orders in the different markets in which they operate. In addition, it is understood as important that a CASP acting as an intermediary should also gather and make available information that attests this effort and ensure that it is available for verification by its customers, market participants and regulators. The recommendations bring significant improvements to the procedures needed to certify compliance with these principles, even in cases in which a CASP is operating in different contexts of competition and rules. Participants also recognize that the recommendations create conditions for reducing possible regulatory asymmetries between CASPs and intermediaries that operate in traditional markets.

- ***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.***

Members agree that there should be limitations in cases where a CASPs exercises both roles (as a market operator and trading intermediary). But **there was no complete consensus on what these limitations should be** - if a total segregation between activities; or if they could occur under the "same roof", however with certain safeguards to mitigate conflicts (as also pointed out in chapter 2 above).

Regarding this issue, the participants observed that in the Brazilian financial and capital markets, regulation determines a formal segregation between trading intermediary and market operator, exchanges and over-the-counter markets. They are different entities and each with their respective responsibilities, regulatory requirements and limitations. This is the form used to mitigate and avoid those conflicts of interest. Part of the group understands that the best way, at least for crypto-assets equivalent to securities. As occurs in Brazilian regulation, there should be **segregation and formal limitations between these activities**. This is because it is understood as an arrangement, like local regulation, as adequate to better deal with the conflicts of interest involved. As well as it avoids regulatory asymmetries between traditional markets and the crypto market.

Nonetheless, another part of the members considers that, in the case of activities related to crypto assets and due their specificities, the limitations to mitigate conflicts would **not need to occur as the same of traditional markets**, where there are certain segregations and prohibitions. The path of the requirements already pointed out by recommendations 4 and 5 would be enough to mitigate and avoid these conflicts. Additionally, there could be additional safeguards and responsibilities proportionate to the identified risks, for example, greater limitations proportional to the total amount of assets involved in the operations of a CASP acting as a market operator and trading intermediary - as pointed out above in the answer of chapter 3 (Question 4).

For a CASP exchange that is also a token market, the members also highlighted the importance of ensuring attestable separation for the specific activity of self-regulation and supervision of its participants, since many entities today do not carry out the proper segregation and present here a source of conflict of interest. Self-regulation and independent internal bodies may also be seem as necessary, since the internal governance and set of incentives that the different areas and businesses the CASP company carries may conflict, and no third-party exists to arbitrate the parties out of the conflict. Such arrangements, and mandatory rules establishing first, second and third lines of defense may also be interesting choices for the regulation of CASPs.

Some participants reminded that in the traditional markets, trading in their own assets (proprietary trade and treasury trade) against positions of clients are also a well-known conflict-of-interest problem that has been mitigated in banks and broker-dealers in many ways: best execution rules, separation and segregation rules, audit tracks, exclusion lists in certain assets, disclosure and pre-approval of trades are amongst the measures traditionally taken. The fact that the blockchain technology made it simpler and more transparent to notice the occurrence of such conflicts promotes the use of the technology - hence the call for avoiding off-chain trades and settlement, which some participants of the group voiced in the discussions had. Mandatory on-chain trade and settlement of transactions may thus be one more item to be added to the list of mitigators.

- ***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?***

Although the group has not formed a position on this matter, an in-depth discussion of aspects related to transactions occurring "off-chain" was considered very important. The importance of greater transparency regarding information related to this type of transaction was reinforced. For example, large volumes of "off-chain" transactions could generate greater fragmentation, making price formation processes more difficult and generating less transparent negotiations.

One way could be to require CASPs to disclose information about "off-chain" transactions – such as the crypto-asset identification; date of operation; nature of the operation (purchase or sale); price and volume. Furthermore, CASPs should carry out this disclosure in a timely manner and with appropriate periodicity to contribute to the transparency of these markets.

4 - RECOMMENDATIONS IN RELATION TO LISTING OF CRYPTO-ASSETS AND CERTAIN PRIMARY MARKET ACTIVITIES

Recommendation 6 – Admission to Trading
Recommendation 7 – Management of Primary Markets Conflicts

- ***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?***

About recommendations on issuer listing activities and crypto-asset admission processes, the group considered the structure suggested by IOSCO appropriate. Participants agree that CASP should be responsible for determining the listing of issuers and admission or suspension of crypto-assistance. They should disclose information about the crypto-asset and its issuer and make public its standards and rules used for these evaluations. These are measures that contribute to the proper functioning of crypto markets and are in line with the standards already followed by traditional markets.

Some participants also voiced the need for more collaboration on the international level to increase the use of mutual recognition, country-of-origin rules, and even the adoption of "pipeline" mechanisms for authorization of assets, CASPs, trading and settlement arrangements. This is because the technology makes crypto assets inherently more prone to internationalization and tradeable across frontiers. Since blockchains may be accessed seamlessly and the truthfulness of trades can be certified from afar, instantly with mechanisms and processes that do not need to rely on the identity of authorized market participants,

alternative frameworks for recognition, supervision and the monitoring of markets and trades are possible and should be encouraged.

They reinforced the importance of greater international standardization and the broader use of mutual recognition mechanisms in the establishment of information disclosure rules. For example, the disclosure of information about the crypto asset and its issuer by CASP seeks to follow some standards already adopted by traditional markets (e.g., prospectuses). Also, best practices for token white papers and technical documents explaining the functioning of certain tokens may be advisable. What could contribute to a better evaluation and comparability by investors. It also helps to harmonize information in cross-border operations.

Some of the members also emphasized the need to use **international cooperation mechanisms for listing assets**, such as the search for greater standardization (a point also connected to the considerations made in chapter 6). Crypto assets are easy and securely transferable in the international level, but the rules under which their trading may occur are not established in many jurisdictions, and may differ quite a lot. Also, although DeFi trading is not being studied in this consultation, one should bear in mind that cross-border trading is becoming very important, with concerns about jurisdiction of regulators in listing too. Experiences in crossborder listings and cooperation between authorities to establish single registration counters could also be undertaken. This is a point of attention and a possible bottleneck given the growing role that multi-jurisdictional listings are assuming.

An additional suggestion would be to evaluate the possibility that crypto assets traded in public markets have an **ISIN (International Securities Identification Number) or equivalent identification**.

- ***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***

The group agrees that, in general terms, no pre-established prohibitions are needed on CASPs listing and/or trading any crypto assets in which they or their affiliates have a material interest. However, **limitations** related to matters such as suitability, market-making activities, disclosure, and conflicts of interest can be required. The group understands that CASPs must ensure that these assets are listed and/or traded on an equal basis with any other assets in their markets. Conflicts of interest in these cases could be mitigated to ensure fair competition between assets, not requiring a ban on listing and/or trading beforehand. As an example, the case in Brazil was recalled, in which the main financial market infrastructure companies, operating in the exchange and over-the-counter environment, have also listed their own proprietary assets.

5 - RECOMMENDATIONS TO ADDRESS ABUSIVE BEHAVIORS

Recommendation 8 – Fraud and Market Abuse
Recommendation 9 – Market Surveillance
Recommendation 10 – Management of Material Non-Public Information

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

Regarding this point, participants noted that, in general, the crypto market would not produce criminal or civil offenses that are unique to these markets or completely new. But, due to specific activities and structures of this market, a greater number of **new actors** could be qualified, allowed, to have certain permissions and accesses that would allow them to commit possible abusive behaviors already identified in traditional markets. Classic fraud, market manipulation schemes and insider information misuse were undertaken by intermediaries and actors related directly to issuers, traders and market operators. Investigation and even the definition of such illicit practices were designed and conform to such patterns. Crypto market abuses, however, are increasingly being perpetuated by coders, suppliers of technology and analysts with almost no direct contact with the traditional market actors. This fact potentially changes investigation tools, distorts legal definitions and legal standard of proof, and may potentially hamper enforcement actions.

Some exemples:

- The crypto market offers new structures and forms of front running, for example, depending on the type of the DLT, its permissions and transparency (such as in public blockchain), the analysis of the chain, flow of orders and their sizes can help create a sense of where the price is going or other information that would allow such abusive behavior.
  - Sandwich attack, a form of front-running that primarily targets decentralized finance protocols and services[4]

[4] As pointed out here: "At its core, a sandwich attack is a form of front-running that primarily targets decentralized finance protocols and services. In a sandwich attack, a nefarious trader looks for a pending transaction on the network of their choice, e.g., Ethereum. The sandwiching occurs by placing one order right before the trade and one right after it. In essence, the attacker will front-run and back-run simultaneously, with the original pending transaction sandwiched in between. The purpose of placing these two orders and surrounding pending transactions is to manipulate asset prices. First, the culprit will buy the asset the user is swapping to — e.g., using LINK to exchange to ETH — with their knowledge of ETH's price increasing. Then, the culprit will buy ETH for a lower price in order to let the victim buy at a higher value. The attacker will then sell ETH at a higher price afterward.". Available here: https://coinmarketcap.com/alexandria/article/what-are-sandwich-attacks-in-defi-and-how-can-you-avoid-them

- Flash Loans, which allows borrowing crypto assets without the need of a collateral. While they have proven popular due to the ease of borrowing, the "weaknesses" present in Flash Loans smart contracts are also used to attack vulnerable protocols. During the short loan period in which there is a change of ownership (governance aspect), the new "owner" of the asset can change its protocol. For example, changing conditions such as price, status of the loan as paid, among others.
- Oracle manipulation attacks, which is related to a manipulation of price oracles that DeFi protocols use to ensure that assets available on their platforms are priced in line with the broader cryptocurrency market and could be also related to flash loans[5].

Additionally, some practices that are currently identified as deleterious to investors may fall short from the traditional definitions of fraud or manipulation. Technological exploits and "back door" practices are more like an *abuse of right* or *abuse of trust*, which distances them from legal standards related to specific patterns required in *fraud* and *manipulation* illicit practices. The qualification as *abuses of right* or *trust* many times make exploits and back doors indistinguishable from legitimate uses or justifiable uses of technological devices. *Intent* and discussions related to legal tests required to frame correctly and prove alleged illegal practices are also meaningful. For example, protocols unintentionally flawed or changes and updates that may be used in exploits are not *designed* to deceive or trick investors into a certain action. Moreover, they may even have been disclosed publicly, and misuse of the protocol on the part of the investor or CASP may have generated the opportunity that led to the questioned loss. Enforcers may, in consequence, fail to present a case to courts or authorities, since the technical elements for fraud or manipulation are missing. It is advisable, thus, that authorities maybe could review their regulatory and legislative frameworks to find better definitions. The recommendation in such cases could be for authorities to ensure the legal framework under which they operate are adequate for administrative and criminal enforcement, with updated definitions of illicit practices and applicable investigation powers.

One of the participants also recalled that it is possible to develop defense protocols, such as creating an upper limit on the price paid for a given asset, to guard against possible attacks. This occurs when trading takes place within the DLT, for example when trading exchanges between two tokens. But these protocols are defense mechanisms that must be raised, a DLT alone does not necessarily guarantee the due protection.

Another participant also pointed out issues related to the protection of personal data. It was pointed out that certain transactions can occur anonymously, allowing certain actions to be hidden. Which also raises the debate about safeguards for a diligent Know Your Customer process.

[5] As also pointed out here: "Bad actors typically carry out oracle manipulation attacks by using large amounts of cryptocurrency to quickly increase the trading volume of low-liquidity tokens on the targeted DeFi protocol, which can lead to fast, significant price increases not reflective of the wider market. Those initial funds are often sourced through a flash loan if the attacker doesn't have the funds on hand. Once an asset's price has been driven up, the attacker can then exchange their artificially inflated holdings for other tokens with greater liquidity and a more consistent value, or use them as (worthless) collateral to borrow assets, never to be repaid. Overall, we estimate that in 2022, DeFi protocols lost $403.2 million in 41 separate oracle manipulation attacks.". Available here: https://blog.chainalysis.com/reports/oracle-manipulation-attacks-rising/

- ***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.***

As we tried to point out above, the group understands that most of the market abuses in the crypto "universe" are already mapped and covered by traditional regulation and surveillance. However, in this new market, there must be greater attention to **what actors can access**, whether new actors, but also broader permissions for already traditional actors.

Regarding additional measures, the group agrees that the framework and actions arising from **self-regulation** could help. For example, through supervision collaboration agreements, such as to review protocols and codes, and support in more operational surveillance tasks. As well as supporting the definition of standardizations, such as scripting and disclosure standards.

6 - RECOMMENDATION ON CROSS-BORDER COOPERATION

Recommendation 11 – Enhanced Regulatory 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?***

The group strongly supports cross-border cooperation amongst authorities and reinforces the importance of these arrangements. A suggestion of possible measures that could strengthen cross-border cooperation could be to reinforce the importance of cooperation oriented by "use cases" or by common issues that must be addressed and have international scope or are of interest to the majority.

A first example of a common issue to be addressed suggested by the group could be actions to strengthen cooperation in cases of **fraud or theft of assets** that generally involve operations in different jurisdictions. For example, cooperation actions that already provide for quick responses to communication actions and necessary measures, such as blocking or unavailability of resources and repatriation of assets. These are actions that are often already foreseen by international entities linked to traditional markets and that could be reinforced or improved for the singularities of crypto markets.

Another potential cross-border project that could trigger a coordinated cooperation movement would be in the direction of facilitating the identification and access of **investors** across different jurisdictions. An application example could be a coordinated and joint effort between jurisdictions for the implementation of a **digital identity in DLT** networks and with arrangements linked to self-sovereign identity, with potential use by individual and legal entity investors. The group points out that solutions of this nature also need to be accompanied by broad debate and standardization measures - already existing and yet to be

established[6]. That is, the group suggests the possibility that the crypto asset markets could raise opportunities to advance on issues that were even previously debated by traditional markets, but which may find facilitations due to the structures and technologies of these new markets. These are complex actions, but they can make use of existing standards and coordination between jurisdictions and through international entities, which can lead to projects with gains in greater efficiency and even inclusion.

Finally, in general terms, the idea of seeking to adapt cross-border structures already used in traditional markets to crypto-asset markets is defended[7].

7- RECOMMENDATIONS ON CUSTODY OF CLIENT MONIES AND ASSETS

Recommendation 12 – Overarching Custody Recommendation
Recommendation 13 – Segregation and Handling of Client Monies and Assets
Recommendation 14 – Disclosure of Custody and Safekeeping Arrangements
Recommendation 15 – Client Asset Reconciliation and Independent Assurance
Recommendation 16 – Securing Client Money 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?***
- ***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.***

[6] An example for legal entities are existing standards, such as the Legal Entity Identifier ("LEI") introduced in 2012 by the G20. The LEI can only be issued by a Local Operating Unit ("LOU") that is certified by the Global Legal Entity Identifier Foundation ("GLEIF").

[7] An example would be to seek appropriate adaptations to the crypto-asset markets of structures such as: (i) national treatment (application of national requirements to any entity that may participate in that market or transaction that may occur in it); (ii) recognition (regulator of a given jurisdiction recognizes third-party regulation as sufficient to meet its own regulatory objectives.); and (iii) passport (set of common rules applicable to the participating jurisdictions guarantees the basis for the creation of a unified market)

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

Regarding this chapter, the group held a broad discussion, which even gave rise to the creation of an Appendix to this document (which seeks to organize different possibilities and paths of tokens to help identify custody measures and issues). In this way, given the complexity of this topic, the group opted to register the main points discussed in general, instead of pointing out specific considerations about each of the questions above required in this chapter.

The group understands the custody service and possible regulatory requirements are of great importance for the proper functioning of the crypto market and for investor protection. Thus, they agree on the pertinence of the recommendations proposed by IOSCO. Additionally, the group reinforced the complexity that the theme assumes in the universe of crypto assets - which we will seek to bring more detail about some aspects.

The group also reinforces that there may be requirements for custody protection proportional to the volume and complexity of the assets held and executed process. Similarly, what happens in traditional markets, such as for credit cards processes, which there are controls depending on the level of processing and resources amounts (e.g., server access control, logical access control, control to be homologated in the infrastructure, among others).

In general terms, the group agrees with the measures to segregate assets to protect the client against the institution's bankruptcy process. Furthermore, they also reinforce the importance of this segregation and internal governance measures also to mitigate the risk of loss, theft, or inaccessibility of client assets. Often these cases occur due to misconduct by members of the custody service provider, so it is also necessary that the measures to avoid these problems are taken and explicitly disclosed. A discussion of best practice could be also positive. For example, no CASP operator, regardless of its position, can move the customer assets alone (e.g., multi-signing solution could be used, so that a few authorized operators must sign off before assets can be moved in and out of the custodian account). In other words, to avoid cases of internal misconduct by CASP, measures to **segregate the client's assets and internal governance** actions are also necessary. These actions should be attestable and for which the due disclosures must be made.

Capital requirements for custody purposes are also important and could occur proportional to the volumes transacted and risks incurred (such as, for example, custody of crypto assets that assume high volatility require a greater volume of capital for the CASP).

Furthermore, the group points out that these measures seek to reduce asymmetries between traditional and crypto markets. So that the regulator does not benefit a certain business model over another (e.g., discussion on segregation of equity vs capital requirements).

About **custody insurance**, the group points out that this is a market issue. However, there may be recommendations for proper disclosure of this service provided, to avoid omission of information or misleading advertising. The group also raised the question whether insurance, even if of a marketing nature, should not be treated as an obligation for the custodian and under what conditions. This obligation would be connected to giving the possibility to the client to contract this insurance or not.

Another point raised is to observe the geographic location of the custody, since this service could occur in

places that generate unavailability of access by the scope of regulation. For example, in countries or jurisdictions with a fragile history of participation in Memorandum of Understanding, international agreements and exchange of information. Or even coil be in contestable areas, such as storage in data canters located in oceans or even satellites.

As pointed out by members, a custody service must provide for: safe custody; reflect transactions; and allow redemption of the asset (return the asset). On this last point, the group pointed out the importance of safeguards or recommendations to prevent the custodian entity from creating impediments or barriers for its client to redeem its own asset.

Seeking to bring more details, the group pointed out that there are some singularities in custody in crypto markets. In this way, some specific precautions must be taken and observed by regulators depending on some characteristics, such as type of asset and DLT network. Examining some of the possibilities and paths that tokens can take (in line with the tentative reflection recorded in the Appendix to this document), the group noted that different paths can generate different levels of risk to investors of losing their assets. Below is a brief attempt to point out different situations and possible risks generated:

Governance in the Network/Smart Contract	
Private/Permissioned Network	low risk (*risk more controllable, manageable*)
Public Network	medium risk

Non-Governance in the Network/Smart Contract	
Private/Permissioned Network	medium risk
Public Network	high risk (*risk less controllable, manageable*)

Native or Non-Native Token	
Native token	Key Custody
Asset-referenced token	Key custody + Asset custody (out of the DLT network and according to applicable laws and regulations of the jurisdiction)

In this way, the possibility of regulatory requirements and safeguards to increase safety should occur proportionally to the observed risks. In which situations that generate greater risk for the investor attract greater requirements and regulatory care, such as safeguards, certifications, greater criteria in approvals, certain requirements for proving procedures and disclaimers.

With regard to custody and risks involved, it is important to observe if there is a governance, whether someone or some agent has full control over the token's life cycle or not (such as mining / minting & burn

issues, transfer, blocking, unblocking, hijacking, avoid \ banish listing, etc. - see also the “Appendix” in this document where the group tried to explore different possibilities). Governance is also related to being able to enforce court decisions on tokens. The point is if there is governance, the group understands the risks of losses for the investor could be more "controllable". Since, ultimately, it is possible to reach identifiable persons responsible in cases of damage to assets and investors, for example. In these cases, robust control measures, systems and safeguards are necessary to guarantee the custody of assets. However, they would be proportionately smaller than scenarios where there is a high risk when there is no governance.

Regarding public networks, where the information is registered on all nodes, there is a higher risk when the presence of governance is not observed. The risks of not having someone or a legal entity to hold responsible for damage or problems with an investor's assets increase. In private or permissioned networks, there is a greater possibility of management and, therefore, the risks are a little lower.

Differences were also pointed out depending on type of the crypto asset:

- Natively digital assets (assets having no analogic or physic counterparty originally issued, recorded, and kept in a DLT-based system) - the key custody is the main issue. And in some cases, the custody could be like what is observed for physical guards (locker, vault).
- Asset-referenced token (in line with the concept brought by MiCA) - here there must also be custody of the key. But attention should also be paid to the custody of the reference asset, which must be immobilized for the issuance of the token. For example, if the token represents a stock in the financial market, the custodian CASP must be required to provide means to prove custody of the reference stock. This measure can be important to guarantee the persistence of the underlying asset and to avoid double spending. Records must reflect the change in ownership.
    - In these cases, it is also important to pay more attention to the legal issues of titulary of assets and the legal regimes of ownership - the regimes of each jurisdiction also to be observed. Regulatory solutions for digital assets must be adequate to the systems operated by the jurisdictions to which they are subject.
    - In these cases, it is also important to differentiate cases in which custody reflects the transfer of ownership / title (authorizing the trading of the underlying asset and/or representative token), from situations in which custody does not authorize.

In the case applicable to private key custodians, they would be responsible for creating and managing the public and private key pairs, that compose the so-called digital wallets. Considering a scenario in which the custody of crypto assets may consist of the safekeeping of the private keys that allow access to the crypto asset, in a given digital wallet, these custodians would be responsible for something similar to a "dictionary of public keys", which references the public addresses to the ownership of the beneficial holder, allowing the regulator and self-regulatory bodies to comply with the IOSCO principle of having comprehensive inspection, investigation and surveillance powers.

With regard to **self-custody**, this implies the possibility of the final beneficiary transferring and storing tokens in a digital wallet that is managed by him/herself. This may imply the impossibility of applying enforcement mechanisms, and even surveillance by regulators, especially in the case of tokens that are of the "non-governance" type, as illustrated in this document in the Appendix, because, in general, these principles are more often applied in their relationship with regulated entities and financial market infrastructures. In the case of "governance" type tokens, which do have governance mechanisms by the token issuer, regulators could have a certain reach, depending on the governance mechanisms implemented.

8 - RECOMMENDATION TO ADDRESS OPERATIONAL AND TECHNOLOGICAL RISKS

Recommendation 17 – Management and disclosure of 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.**
- **Question 18: – Are there particular ways that CASPs should evaluate these risks and communicate these risks to retail investors? If so, please explain**

In general, as pointed out above, for the group, the structures and activities of crypto markets do not necessarily bring completely new operational and cybersecurity risks. But the possibility of different and new actors having access and possibilities of action that increase the risk of these events. For example, a certain operator having access to a wide range of information and becoming the target of a cyber-attack.

Again, the participants recalled the question about the physical location of certain network services, so that attention should be paid to locations in countries or areas where there are complications for regulators to reach.

Members also highlighted the feature of DLT networks where there is no possibility to reverse transactions. In this way, it can give rise to operational solutions that must resort to arrangements outside the network so that a reversal of a transaction occurs.

Additionally, certain smart contract codes may allow changes, or upgrades, which may represent gateways to operational and cybersecurity risks. Another point is to seek, as noted above in the custody section, would be to create mechanisms to prevent only one person from holding the private keys of the exchange accounts (eg CEO of the CASP or others) - thus avoiding cases of theft, loss of keys, or even cyber-attacks targeting these people (such as phishing).

With regard to external audits, the group pointed out the need for greater training and knowledge of its agents. It is often the audited entities that explain technical concepts to the audit representatives, thus offering a risk of misconduct in these interactions and with that certain threats are not perceived by the audits. A standard followed by auditing companies was not observed, making it difficult to comply with the requirement and formation of good common practices.

9 - RECOMMENDATION FOR RETAIL DISTRIBUTION

Recommendation 18 – Retail Client Appropriateness and Disclosure

- **Question 19: – What other point of sale / distribution safeguards should be adopted when services are offered to retail investors?**
- **Question 20: – Should regulators take steps to restrict advertisements and endorsements promoting crypto-assets? If so, what limitations should be considered?**

The group agrees and reinforces the importance of the recommendations pointed out by IOSCO. The participants only indicated a special attention to the following points. First, measures to prevent a CASP from creating too many barriers and difficulties for a retail customer to close their account. In general, this possibility must be done through the same channel and with the same ease in which the account was opened.

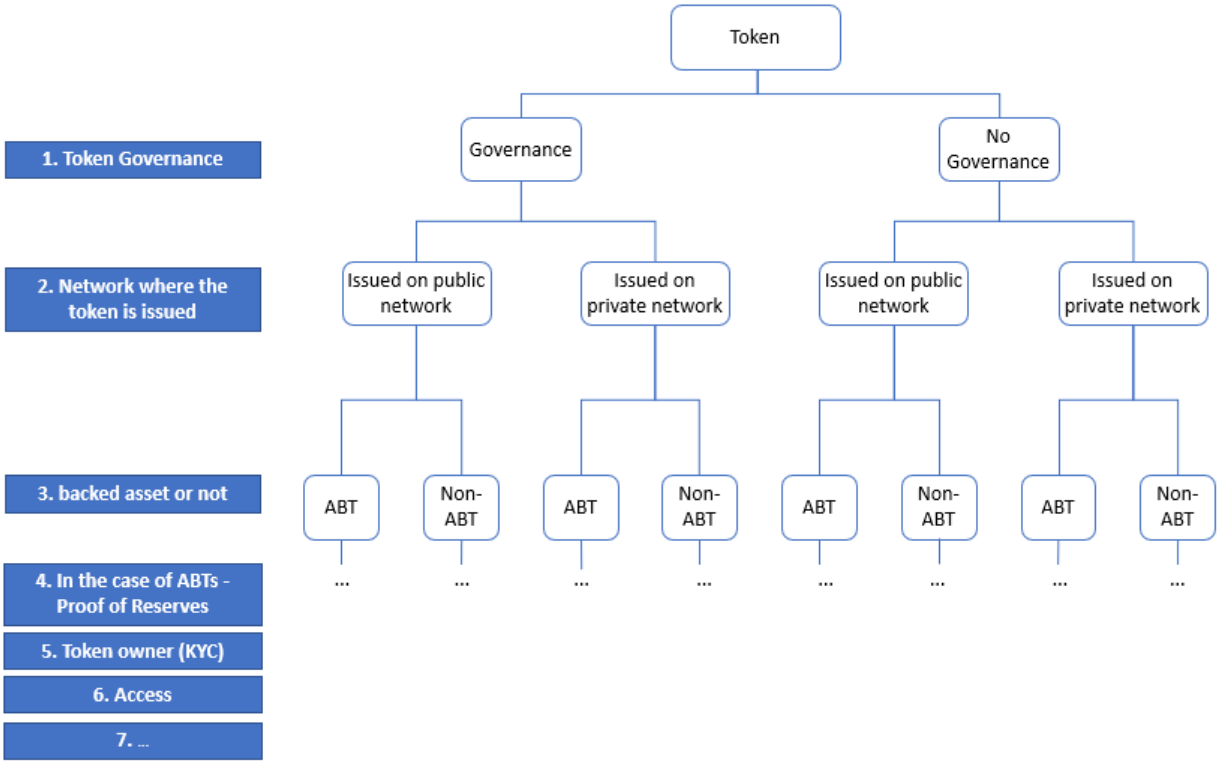
The group also highlighted the growing importance of social media as a source of information about crypto assets and the increase in the number of retail investors who follow financial influencers. It should be noted that it is necessary to promote transparency. One path would be to look for ways to ensure that influencers reveal their contractual ties with CASPs when offering sponsored content related to crypto assets. For example, establishing minimum measures and rules for influencers to inform investors that it is an advertisement, disclosing their contractual relationship when offering sponsored content and even disclosing remuneration conditions and influencer commissions. In these cases, the digital influencer did not become a regulated participant, but the responsibility would fall on the regulated CASP. The group recalled that, depending on the case, the recommendation of an influencer can even be seen as market abuse, for example, when it ends up generating movement in asset prices and benefiting certain groups linked to these movements.

Participants also pointed to the risk of a dusting attack and impacts for retail investors. The dusting attack is an attack in which a trace amount of crypto, called dust, is sent to wallet addresses. However, there are some FinTech's and service providers that replicate, especially for retail investors, strategies from certain reference portfolios. In this way, when there is a dusting attack on one of these reference portfolios, it generates the effect that retail investors that replicate reference portfolios automatically also buy these implanted assets, which often lack real value.

APPENDIX: "*Token decision tree*"

In addition to the answers to the consultation questions, the group also discussed different possibilities observed for crypto-assets and possible still open questions for its members. An effort (*initial draft and not exhaustive*) was therefore made to try to organize the different situations observed – what was called by the group the "token decision tree". We have recorded this draft here. It deals with an attempt at a generic and modular organization of possibilities. The objective was to map different ways that tokens can take and possible ramifications that could configure points of attention for greater attention from the regulators.

Figure 1: Draft of the "Token decision tree"



Source: own elaboration.

1. **Token governance:** Whether someone or any responsible agent has full control over the token's life cycle or not (e.g., mining / minting & burn, transfer, blocking, unblocking, hijacking, avoid \ banish listing, etc.), including being able to enforce court decisions on tokens.
2. **Network where the token is issued**: If a token is issued on more than one network, it can be analyzed on a case-by-case basis.
3. **Regarding backing**: If the token is backed by an asset (ABT – Asset Backed Token) or it is not backed by an asset (Non-ABT). Or could be the difference between "*Asset-referenced token"* and "*Natively digital assets",* as pointed out above in chapter 6.

4. **In the case of ABTs, regarding the existence of Proof of Reserves**: Whether ABT has proof of reserve or not. Additionally, whether the proof of reserves is audited or not, continuously monitored 24x7x365 or by sampling. Note: Non-ABTs would not have this branch.
5. **Owner of the token (KYC)**: Whether the owner of the token is fully identified or not.
6. **Regarding access**: Whether the token is universal or restricted. This depends not only on the geographic scope of the network, but also on who can access it. Eg: some token was issued on the Ethereum network (global), but only investors from certain locations could acquire it.
7. Other possibilities (other “leaves” and “branches”) …

Examples of "leaves". Ex.:

- No governance → Token issued on public network → Non-ABT → No borders → Token owner identifiable or not → ... = bitcoin, ether
- with governance → Token issued on public network → ABT → Without borders → Token owner identifiable or not → ... = USDT (Tether dollar), USDC

The attempt to organize the possibilities above occurred to support the group's debates, but it also opened additional questions which we record below. Open questions (non-exhaustive list):

(1) **Order of branches**: what is the best sequence? Which ones make the most sense? The idea is that the tree helps to understand important issues related to crypto assets. It is modular according to the question or issue to be analyzed (like a "lego"). In this case each branch is binary, with “leaves” (options) but could have more options. The decision tree can be asymmetrical in case some branches do not make sense.

(2) **Ramifications and possible doubts and issues**:

- Whether the token has bridges to other networks or not (may imply token custody or not, double spend and cybersecurity)?
- Whether the token can be used in DeFi or not (may imply token custody or cybersecurity issues)?
- Whether the token has a secondary market or not?
- Does the token have finite or unlimited stock?
- About whom can custody the token: self-custody x delegated to trusted third parties x both.
- About the token owner's KYC responsibility: token issuer x wallet issuer x trading platform (e.g., crypto exchange). Motivation: In the case of bitcoin, it is not possible for the token issuer, in this case the network / miner, to KYC the wallets. In the case of the primary market of a manageable token, it may be the responsibility of the issuer or the platform.
- Would this organization be useful for delimiting borders, identifying risks and defining the regulatory perimeter? Ex.: Central Bank / Monetary Authority x Securities Commission x other x Undefined
- Other definitions?

(3) **Evaluate the "navigation" in each branch and possible reflections and consequences from it** (whether it makes sense or not, what risks are involved in the possibilities, what responsibilities, if the token or possibility should rise to the possibility of being regulated or not, if you have to have insurance or no, questions of suitability or not, etc.). Operationally, this "tree" may give rise to reflection on the consolidation of a taxonomy for the crypto-asset markets, greater delimitation of concepts and borders. As well as developing the possibilities of this tree for a more detailed analysis of the functions present there, associated risks and needs for regulatory measures. One way to do this would be to develop the tree, number the final “leaves” of the tree and place them in a table, in a grouped way. Ex.: Sheets 1, 2, 3, 17 and 15 need prior regulatory authorization and suitability analysis. Sheets 20, 21 and 22 are prohibited (e.g., ABTs without proof of reservation, issued on public networks, universal and without KYC, due to risks of illicit acts.)