The Board of the International Organisation of Securities Commissions
C/ Oquendo 12
28006 Madrid
SPAIN
By email: cryptoassetsconsultation@iosco.org

28 July 2023

Public Comment on IOSCO’s Consultation Report on Policy Recommendations for Crypto and Digital Asset Markets

Dear Sir/Madam,

Binance welcomes the International Organisation of Securities Commissions (IOSCO) work on Crypto and Digital Asset Recommendations. This work was addressed to relevant authorities looking to support jurisdictions seeking to establish compliant markets for the trading of crypto or ‘digital’ or ‘virtual’ assets in the most effective way possible.

The industry is spread across jurisdictions, and disintermediates financial services using technologies that operate across the globe 24/7, with less emphasis on traditional supervision structures. Given this, the importance of global standards increases. The ideal regulatory response should be coordinated, consistent and comprehensive. Regulation must be proportionate to the nature, scale and complexity of the risks.

Our detailed response is attached, however we highlight the following key points:

- We support IOSCO’s work to prevent regulatory fragmentation or conflicts across markets and borders globally by using high-level, outcomes focussed principles that promote consistency and certainty for operators.
- Cross-border cooperation and coordination is important given the borderless, global nature of digital and financial markets. However, there is an increasing need to modernise the existing regulatory framework for financial markets globally, and to ensure current approaches remain fit for the digital age by making this process quicker with a premium placed on principles over process. This includes IOSCO leading on reforms necessary to enable responsible disintermediation.
- Binance is supportive of effective, credible and proportionate measures to prevent market abuse and enhance integrity. Consistent with other industries and regulated sectors, criminal or civil offences should be part of a broader regulatory continuum designed to deter illegal activity and achieve good regulatory outcomes.
- It is recommended that regulators work collaboratively with trade repositories, approved reporting mechanisms (ARMs), and approved publication arrangements (APAs) to support crypto exchanges in fulfilling their transparency obligations under e.g. MiFID II.
- We disagree that Crypto Asset Service Providers (CASPs) should be prohibited from listing or trading crypto assets in which they, or their affiliates, have a material interest. As long as there is sufficient governance in place to mitigate conflicts of interest, including appropriate disclosure, transparency and separation of market makers away from the exchange, it should be allowed.
Where multiple activities subject to regulation (such as custody or a broker dealer) coexist within a regulated crypto asset trading venue, they should be supported by robust governance, effective risk procedures and adequate internal and external control mechanisms.

- We would suggest looking at Lloyds markets or insurers methods of rating a custodian’s security overall and have custodians or ‘ratings’ agencies independently provide this score to clients and regulators (i.e. A+ etc).

- There is a need for a collaborative effort between government and CASPs to develop a Risk Assurance Framework which can assure all parties in a transparent and appropriate manner. In lieu of an industry standard for CASP assurance, there are many industry standards that can be achieved and demonstrated (ISO certifications, SOC, PCI DSS, Cyber Essentials +, CBEST Open Source Security Audits).

- As the market in trading and listing crypto assets matures, some form of advertisement and endorsement regime is helpful. However, due to the inherent cross-border nature of crypto services, restrictions on crypto-advertisements should not hinder the free provision of crypto-services on a cross-border/multi jurisdiction basis.

Finally, given the significance of the proposals on the industry, we would appreciate the IOSCO undertaking roundtables to discuss feedback, as the recommendations are finalised.

Please do not hesitate to contact us if you have any questions about our response or require any further information.

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

No, these appear consistent with the lifecycle approach. We agree that the primary intent of the proposed recommendations should be principles-based, outcomes-focused and aimed at the activities performed by crypto-asset service providers (CASPs). As such the recommendations should:

- focus on the regulated ‘service’ or ‘activity’ in scope of IOSCO and its members remit, and not regulate the underlying crypto itself where its use is not within scope of financial services regulators;
- ensure consistency with respect to how global standard setting bodies and IOSCO members approach the regulation and oversight of crypto-asset activities;
- provide clarity and certainty for affected parties, recognising that groups may be affected differently;
- be risk-based and proportionate to the nature, scale and complexity of the risks inherent in the business model and the activities of the firm; and
- avoid duplication or conflict with other existing or proposed regulations.

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?

Yes, regulation is an important part of the lifecycle of all innovative sectors. The foundation of such a regulatory framework must be built on basic principles to maximise protections for users by fostering a safe, secure and sustainable digital ecosystem, while fostering innovation.

We agree that regulators should take an outcomes-focused approach based on high-level regulatory recommendations or principles tailored to the specific attributes of crypto assets. Copying and using existing rules is likely to present operational challenges as the benefits, risks and opportunities may differ due to the nature of the technology and the manner in which the activities and services inherent in the crypto asset and digital ecosystem are provided.

For example, the nuances of certain activities such as decentralised finance (DeFi), which relies heavily on innovative technology such as smart contracts, needs to be properly accounted for. Additionally, crypto-asset markets operate 24/7/365, therefore traditional practices such as standard daily margin call and settlement after the market closes, or controls such as circuit breakers, do not work in the traditional sense.

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?

We agree that users should be able to access information relating to the roles and capacities of a CASP. This information should be transparent, relevant, targeted and proportionate to the risks that may arise from a CASP’s activities.

We agree that in-scope regulated entities considered to be “vertically integrated” or “agglomerated” should be expected to follow rules relevant to those regulated activities – not just those relevant to operating a crypto asset trading venue. Where multiple activities subject to regulation (such as custody or
a broker dealer) coexist within a regulated crypto asset trading venue, they should be supported by robust governance, effective risk procedures and adequate internal and external control mechanisms. This includes appropriately segregating those activities within the same group structure rather than limiting corporate groups to providing only specific ring-fenced services.

However, legal separation of activities of CASPs undertaking a variety of services similar to traditional financial services may not be necessary to achieve segregation of risks in practice. This is partly because the inherent characteristics of CASPs, and the underlying technology used, may require a different approach to regulating them compared to traditional financial entities.

For example, custodian regulation should allow for a dedicated corporate entity within the group structure of the CASP, with appropriate insolvency ring-fencing measures for wallets, to safeguard users’ assets. Otherwise, depending on the business or customers of the CASP, this would require double licensing of exchange and custodian and render settlement between the wallets of those legal entities impracticable. For example:

- it may not always be operationally feasible (and may in fact increase security risk) where a third party custodian is required to hold customers’ assets;
- the CASP may list a wide range of tokens, some of which third party custodians may not be capable of holding,
- involving a third party custodian may require on-chain transfers which may compromise security, timeliness of transfer and increase cost to users.

**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?**

We agree that managing conflicts of interest, including the drafting of a conflicts of interest register and the management of such for a regulated entity and its Board is necessary. As per question 3 above, we believe that robust governance, effective risk procedures and adequate internal and external control mechanisms are an alternative to costly and inefficient segregated legal structures and operations. As the industry and technology continues to mature, disproportionate regulation may inadvertently stifle innovation and growth, remove choice and competition, and potentially drive consumers to unregulated markets or operators. As such, industry and regulatory collaboration is vital to identify credible solutions and address such risks proportionately for the benefit of all.

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

Yes, however it is important to note that the inherent characteristics of crypto and digital asset markets, and the underlying technology used, may require a different approach to regulation compared to traditional financial entities. For example, in some scenarios, e.g. clearing and settlement and options and futures, regulated crypto and digital asset service markets may operate quite differently to traditional financial markets. This is both practically, in terms of process and technology, and operationally in relation to daily settlement and hours of business, requiring a more nuanced approach relative to traditional finance.
Question 6: What effect would Recommendations 4 and 5 have on CASPs operating as trading intermediaries? Are there other alternatives that would address the issue of assuring that market participants and clients are treated fairly?

We support fair, orderly and transparent markets for the trading of crypto assets.

For recommendation 4:
- Orders executed using Central Limit Order Books (CLOB) should be done on a first come first out basis (FIFO).
- Best execution should be implemented for the benefit of both professional and retail clients using market intermediaries with sufficient knowledge and expertise.

For recommendation 5:
- Current transparency requirements for regulatory reporting are designed for large-size and relative low trading volume counterparties. However, many crypto asset traders are individuals and tend to trade small quantities with large volumes of orders.
- It is recommended that regulators work collaboratively with trade repositories, approved reporting mechanisms (ARMs), and approved publication arrangements (APAs) to support crypto exchanges in fulfilling their transparency obligations under e.g. MiFID II, despite extremely high transaction volumes. This would foster a cost-efficient reporting environment, which may include more streamlined reporting lifecycles, or the provision of more cost-effective services.
- Existing transparency reporting requirements (such as EU MiFID) will be very costly for crypto asset firms due to the sheer volume of trades and traders, potentially impacting the trading systems performance. These costs can be particularly prohibitive for new entrants, thereby limiting market competition and stifling innovation.
- The current expectations for transaction reporting may also need to be reconsidered in light of the global nature of crypto-asset trading. In numerous jurisdictions, entities are required to report transactions where a counterparty is located outside of the local jurisdiction: a requirement that significantly increases the regulatory burden for international CASPs. This is particularly problematic where clients value anonymity. A potential solution could involve industry use of Privacy Enhancing Technologies, provided that the CASP can disclose the true identities of these counterparties to regulators upon request.
- Different regulatory regimes have different specifications meaning the cost and complexity of reporting reflects the need to maintain multiple reporting engines globally. We would encourage greater regulatory harmonisation and coordination in this area.

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.

We believe CASPs should be allowed to engage in both the role of market operator and trading intermediary but only if they are segregated, with effective controls to prevent conflicts of interest. For example, to effectively mitigate any potential conflicts of interest CASPs should:

- adhere to a set of principles and operational requirements designed to maintain a level playing field
- adopt best execution practices requiring CASPs to take all necessary steps to achieve the best possible trading outcomes for their clients
• ensure proprietary trading activities conducted by entities in the same group as CASPs do not disadvantage other participants through enforced regular audits and independent reviews of CASPs’ trading operations
• segregate client assets from those used for the CASPs’ own trading activities to insulate client assets from potential losses resulting from entities conducting proprietary trading in the same group as CASPs
• implement distinct identifiers for reporting their market-making and trading activities. This would provide regulators with a clearer picture of the CASPs’ functions and enable more effective oversight

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

As per Q7, both pre and post-trade transactions should be visible to regulators and reported (with a reasonable delay built in). Binance’s pre and post-trade transactions on its CLOB are already available for disclosure. Regulators may also wish to consider introducing a crypto asset classification flag to the reporting process to help identify and distinguish both styles of booking.

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

Binance already has a comprehensive listings process in place that includes the items identified. Taking into consideration the unique nature of crypto assets, their significant trading volumes and global accessibility it is important to establish a regulatory framework that allows CASPs to swiftly manage the listing and delisting of these assets.

CASPs should be primarily responsible for determining whether a crypto asset is admitted to trading. It is also important to ensure appropriate regulatory oversight of the admission process to trading crypto assets on exchanges and this could be achieved in different ways e.g.:

• Self-certification: Under this route, prior to admitting a new crypto asset to trading the exchange would self-certify to the relevant competent regulator that the virtual asset it intends to list is a crypto asset within the relevant definition, and that the crypto asset has met the CASP’s requirements for listing. The regulator would then have an opportunity to stay the listing within a prescribed time period.

• Review and approval: Under this route, an exchange may instead request the relevant regulator review and approve a particular crypto asset for admission to trading rather than the exchange undertaking a self-certification process.

Regulators could also publish a list of all crypto assets submitted to it under either route. The publication of such a list would provide certainty to the industry regarding which crypto asset products are deemed to be regulated. This would be of particular assistance to new or developing exchanges and would provide users with additional comfort that the crypto assets they are buying or selling are regulated products.

Operationally we would identify the following additional points for IOSCO to consider:
- what information should be submitted by a crypto asset issuer for admission to trading e.g. “whitepaper”, bearing in mind that whitepaper content requirements should be aligned as much as possible across jurisdictions
- the level of due diligence to be undertaken by the exchange in respect of key risks such as the background of the issuer of the crypto asset, product roadmap, tokenomics, finances, code design and infrastructure security
- acceptable processes for the orderly delisting of a crypto asset
- regulatory resilience when crypto-asset markets operate 24/7/365, requiring a reconceptualisation of regulatory oversight. Traditional regulatory bodies will need to consider the demands of such market activity, which extends beyond conventional working hours and often intensifies during weekends and public holidays.

**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.

We disagree that CASPs should be prohibited from listing or trading crypto assets in which they, or their affiliates, have a material interest. As long as there is sufficient governance in place to mitigate conflicts of interest, including appropriate disclosure, transparency and separation of market makers away from the exchange, it should be allowed.

Crypto markets, in their current form, play a significant role in nurturing and financing innovative projects. By providing much-needed liquidity, these markets act as catalysts for the growth of projects exhibiting high potential. Placing limitations or prohibitions on CASPs listing or trading any crypto-assets in which they or their affiliates have a substantial interest could potentially stifle innovation. Before entering the market, many burgeoning projects rely on this liquidity infusion to provide financial support. Without such support, these limits constrain liquidity and order book depth. This may lead to wider spreads and may negatively impact the public.

As an example, we refer to BNB. BNB is a cryptocurrency (token) and the native asset on BNB Chain, a decentralised blockchain software system. BNB has many use cases outside of Binance Exchange, including payments, travel, gaming, and entertainment. BNB and BNB Chain are supported by a decentralised community of users, developers, validators and delegators. Binance does not control or operate BNB Chain or BNB, and BNB is not related to the profits of Binance or an investment in Binance. Many exchanges other than Binance also allow users to buy and sell BNB.

If regulatory action were to restrict these markets, the repercussions could be detrimental for the continued evolution of blockchain technology and the broader crypto-asset ecosystem. Without the liquidity offered by these markets, there may be insufficient incentives for the development and proliferation of promising technologies.

**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.

The market abuse behaviours specified in the consultation paper cover most cases and Binance is supportive of effective, credible and proportionate measures to prevent market abuse and enhance
integrity. Consistent with other industries and regulated sectors, criminal or civil offences should be part of a broader regulatory continuum designed to deter illegal activity and achieve good regulatory outcomes.

The management and mitigation of risk relating to market abuse and integrity should also consider direct enforcement against individual clients without affecting markets and a more holistic approach relating to addressing online harms caused by social media and key opinion leaders / influencers.

However, there are scenarios unique to crypto markets that require greater coordination across the public and private sector to resolve. Examples that may require new or existing criminal or civil offences to be more rigorously applied include:

Account Takeover (ATO)/Crypto Theft: This involves unauthorised access to crypto wallets or exchanges. Once the attackers get access, they may engage in a variety of nefarious behaviours such as stealing digital assets, compromising personal information, or utilising the account to launch more attacks.

Fraudulent Initial Coin Offerings (ICOs): ICOs are fundraising techniques in which new cryptocurrencies are made available to investors. Scammers may create fake ICOs that promise large profits before disappearing with the funds acquired. This form of fraud has the potential to fool investors and destroy the integrity of the crypto market.

Unregistered Tokens Offerings: Some crypto exchanges operate without proper registration or compliance with regulation of Token Offerings. This can put investors at risk and jeopardise market integrity.

**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.

We agree that robust market surveillance policy and tooling are necessary to identify market abuse risks and operate the market. As the crypto market is global, operating 24/7/365 it is difficult to suspend a market by focusing on one operator whilst other operators remain open impacting the global price.

Due to the particular characteristics and challenges of the crypto market, extra measures to improve the existing surveillance programme, some of which are currently under consideration by policymakers, are required. For example:

- Collaboration and information sharing: Collaboration among regulatory agencies, exchanges, and other relevant parties is critical. Sharing knowledge and best practices can aid in the identification of emerging threats and the enhancement of surveillance capacities e.g. new crypto-assets, suspicious transactions and known bad actors. We would highlight for consideration the need to refresh MoUs and agree cooperation agreements with regulatory peers globally. This can take time and should be prioritised through supranational entities involved in global policy making.
- Market transparency: Improving market transparency in the crypto market can aid in the identification and prevention of market abuse. Measures such as requiring exchanges to disclose near real-time transaction data, promoting pricing transparency, and ensuring accurate trade volume reporting might all lead to a more transparent and accountable market.
- Continuous monitoring and adaptability: As the crypto market evolves, the market surveillance
requirements must be updated and amended on a regular basis to cope with novel risks. Continuous monitoring of market trends, technical innovations, and regulatory changes supported by future-proofed regulatory principles is required to guarantee that detection methods remain successful.

**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?**

Cross-border cooperation and coordination is important given the borderless, global nature of digital and financial markets. Across the globe existing financial markets are supervised by various regulatory bodies with their primary focus on supervising their respective industries based on the remit of these regulators. These regulatory bodies tend to be structured on historical activity-based lines covering banking, which includes payments, securities and insurance. Similar structures can be observed at regional levels e.g. APAC, EU, LATAM, and domestically at the country level. This approach is consistent with the ‘same activity, same risks, same regulatory outcome approach’ with the various bodies at the global level seeking to coordinate their membership, achieve consistency globally whilst avoiding arbitrage across countries.

However, there is an increasing need to modernise the existing regulatory framework for financial markets globally, and to ensure current approaches remain fit for the digital age by making this process quicker with a premium placed on principles over process. IOSCO member countries that have consumers who are unbanked, de-risked or excluded from traditional financial services due to technology, commercial or other factors beyond their control, should be prioritised, empowered and supported by IOSCO. This includes IOSCO leading on reforms necessary to enable responsible disintermediation. Where reform is lacking, politicians and consumers across the globe will increasingly demand change.

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

We support customer protection and asset security. As such, we invest in compliance solutions that cater for specific requirements such as the EU’s new MiCA rules on asset segregation. We also support IOSCO’s work to prevent regulatory fragmentation or conflicts across markets and borders globally by using high-level, outcomes focussed principles that promote consistency and certainty for operators. Applied correctly across markets, high-level principles help firms plan ahead with confidence and certainty when, e.g. drafting their terms and disclosures, designing custody and segregation solutions, and implementing day-to-day solutions for the benefit of consumers and markets.

In striving to ensure adequate protection for client assets, IOSCO may wish to consider how it can achieve proportionate outcomes related to “foreign jurisdictions”. This may avoid competing claims involving different country regulators by clearly defining home and host state powers in the case of cross border provision of services. IOSCO may also wish to help address the challenges CASPs face when engaging suitable audit firms to meet audit requirements. IOSCO should also consider supporting solutions for third-party crypto asset custodian insurance markets, and the development of independently managed and custodied insurance pools similar in operation to investor protection schemes. Irrespective,
custody solutions should be practical whilst ensuring risk-based and proportionate security and safety for customers and platforms.

**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-asset 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.

(a) For the reasons given in question 14 solutions at the country level should reflect IOSCO’s global, principles-based, outcomes-focussed approach and avoid prescriptive and overly restrictive measures.

(b) As per (a), prescriptive and overly restrictive measures risk being misaligned with IOSCO’s proposals and may inadvertently impact new technological and other developments affecting the safeguarding of customer crypto-assets.

(c) This is a highly technical question, but we would highlight the Merkel Tree/zk-SNARK method for proof of reserves proposed by Vitalik Buterin and implemented in the Binance Proof of Reserves (POR) system as one solution intended to safeguard client assets in the way described. The POR solution is new and innovative but is particularly well aligned with the crypto ethos of transparency and trustlessness. It also illustrates how new technology and innovation from the crypto asset industry can evolve from a proof-of-concept to something that can potentially help consumers and industry, including in the traditional securities markets.

(c) (d) Terminology and jargon such as Hot, Warm, Cold are weak terms that give a false sense of security. A badly implemented cold solution is far more insecure than a strong hot solution so we would not assume cold is always ‘better’. We would suggest looking at Lloyds markets or insurers methods of rating a custodian’s security overall and have custodians or ‘ratings’ agencies independently provide this score to clients and regulators (i.e. A+ etc). IOSCO may also wish to consider how to ensure a globally consistent approach to other crypto asset related matters such as ring-fencing from other group entities, bankruptcy protection (of custodian and any 3rd-party providers), contingency and resilience solutions (i.e. identification of other custodians that can hold the clients assets or hold backup / recovery keys / shards) when the primary encounters a negative event.

(c) (d) In the context of recommendation 16 we would propose submission of data to the home regulator on Net Asset Value with pricing in the jurisdiction’s base currency both at aggregate and client level. This would enable clients and regulators to identify if the ratio of capital / third-party insurance / other security funding (such as self-funded insurance solutions), relative to the actual assets held, is above or below their risk tolerance and take action appropriately. As crypto asset custodians increasingly become financial market infrastructure this will help to protect client, market and regulator reputations. Such
procedures will also be useful for the monitoring and management of collateral in lending transactions (e.g. margin), including in liquidation scenarios.

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

Client asset protection is vitally important and we agree that client assets need to be adequately safeguarded. There are many legal and technical matters to be worked through as the industry and technology matures but adequate safeguarding of client assets needs to be at its heart. Matters for consideration include:

- how client and proprietary assets are appropriately stored, segregated, identified and accounted for when the crypto assets are less tangible and easier to move digitally.
- operational aspects such as on-chain and off-chain segregation, and how to account for non-native token movement costs when the CASP incurs gas/fees, including whether such costs are passed back to clients or absorbed by operators.
- what legislation, or other requirements, exist in countries to support adequate protection of client assets, including in areas of property and insolvency law, irrespective of common or civil law structures.
- how to ensure adequate mitigation of people, policy, procedural, and technology risks. This includes considering key generation, storage, nodes and signing events as all hackable. Custodians should also be expected to meet commonly accepted international standards related to risk management e.g. ISO that focus on all angles of risk, not just cyber 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.**

The risks posed to a CASP are higher than that of a traditional financial services provider, therefore the risk landscape is entirely different and requires a new lens in order to accurately ascertain and manage risk in relation to digital assets. Fundamental security concepts apply when CASPs are evaluating adequate and effective technology and cyber control measures. However, there is little room for risk acceptance in basic controls risk management when digital assets are within the institution's area of responsibility. In addition to ‘excellence’ in fundamental controls, a level of assurance akin to that seen within tier one financial institutions’ controls validation exercises is required, e.g. CBEST. Such controls testing is required for a CASP to accurately understand the risk level from a pragmatic and ‘deep dive’ approach to effective risk management. Such cyber controls are modern cyber threat management methodologies rather than cyber technologies.

In addition to the above relevant comments, any operations on the blockchain are irrevocable. For example, if the asset destination is incorrectly entered the asset will be lost.
Question 18: Are there particular ways that CASPs should evaluate these risks and communicate these risks to retail investors? If so, please explain.

CASPs could consider the external validation of industry best practice to ensure that appropriate safeguards are in place to protect the digital assets under management and include a public page highlighting such credentials so that the user base can validate assurance. Considerations of what would be deemed appropriate for assurance are varied and cover a wide range of possible validation measures to demonstrate to users that trust has been achieved within the control framework of the CASP. In lieu of an industry standard for CASP assurance, there are many industry standards that can be achieved and demonstrated (ISO certifications, SOC, PCI DSS, Cyber Essentials +, CBEST Open Source Security Audits).

There is a need for a collaborative effort between government and CASPs to develop a Risk Assurance Framework which can both assure all parties in a transparent and appropriate manner.

For withdrawal addresses that are known or suspected to be scams, Binance uses pop-up warnings to protect our users.

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

We agree that some of the traditional retail financial markets tools could be considered for relevant in-scope cryptoasset products or services. This could include:

- client suitability assessments taking into account the difference in the complexity of the underlying product or service that is being offered.
- product knowledge assessment/appropriate testing developed with the support of the industry to ensure that retail clients understand the risks involved and have sufficient knowledge.
- responsible trading pages and self-control functions where relevant and proportionate.

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

Yes, as the market in trading and listing crypto assets matures, some form of advertisement and endorsement regime is helpful. Particular areas of weakness relate to how crypto assets may be marketed or endorsed by unregulated third-parties as speculative gambling type products. We suggest a solution should be applied in a manner consistent with the “fair, clear and not misleading” principle, based on the nature of the customer and of its business. This would also help support some form of liability regime modelled on existing legal precedent.

However, due to the inherent cross-border nature of crypto services, regulators should maintain a level playing field when imposing restrictions on crypto advertisements. Restrictions on crypto-advertisements should not hinder the free provision of crypto-services on a cross-border/multi jurisdiction basis.
Question 21: Are there additional features of stablecoins which should be considered under Chapter 10? If so, please explain.

We would support:

- wider development of accepted audit solutions that enable stablecoins to be audited externally to ensure they are backed with the assets claimed.
- greater clarity of KYC obligations on the issuer of a stablecoin in respect of holders in two tier models.

At present, most fiat-backed stablecoin arrangements operate in a tiered model, in which the majority of users do not have a direct relation with the issuer. Instead, they buy and sell the tokens on secondary exchanges, which have subjected them to KYC requirements. Tiered arrangements ease the operational burden on issuers (e.g. the burden of onboarding of clients and processing redemptions) and mitigate risks by distributing them through a number of regulated intermediaries. Furthermore, consumers can choose from a range of intermediaries to effectively convert their stablecoins back to Fiat. Holders should always be given the choice to enter into a direct relationship with the issuer and redeem directly from them at par, but the issuer should not be required to onboard each and every client unless, and until, the client decides to exercise that right.

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

Private key holder risks:
We highlight the need to consider appropriate policies and procedures for CASPs to ensure that client and company funds are not subject to single point of failure risks. For example, having risk management controls for the storage of private keys and for the key generation process are critical to safeguard private keys. As such, we want to suggest the use of Multi Party Computation (MPC) in key generation, which is a mechanism to generate and split the private key into multiple pieces distributing them in multiple places and storing them securely so that no one person will have full access to the private key. This methodology, in our view, has superior risk controls compared to the traditional method of creating private keys.

---