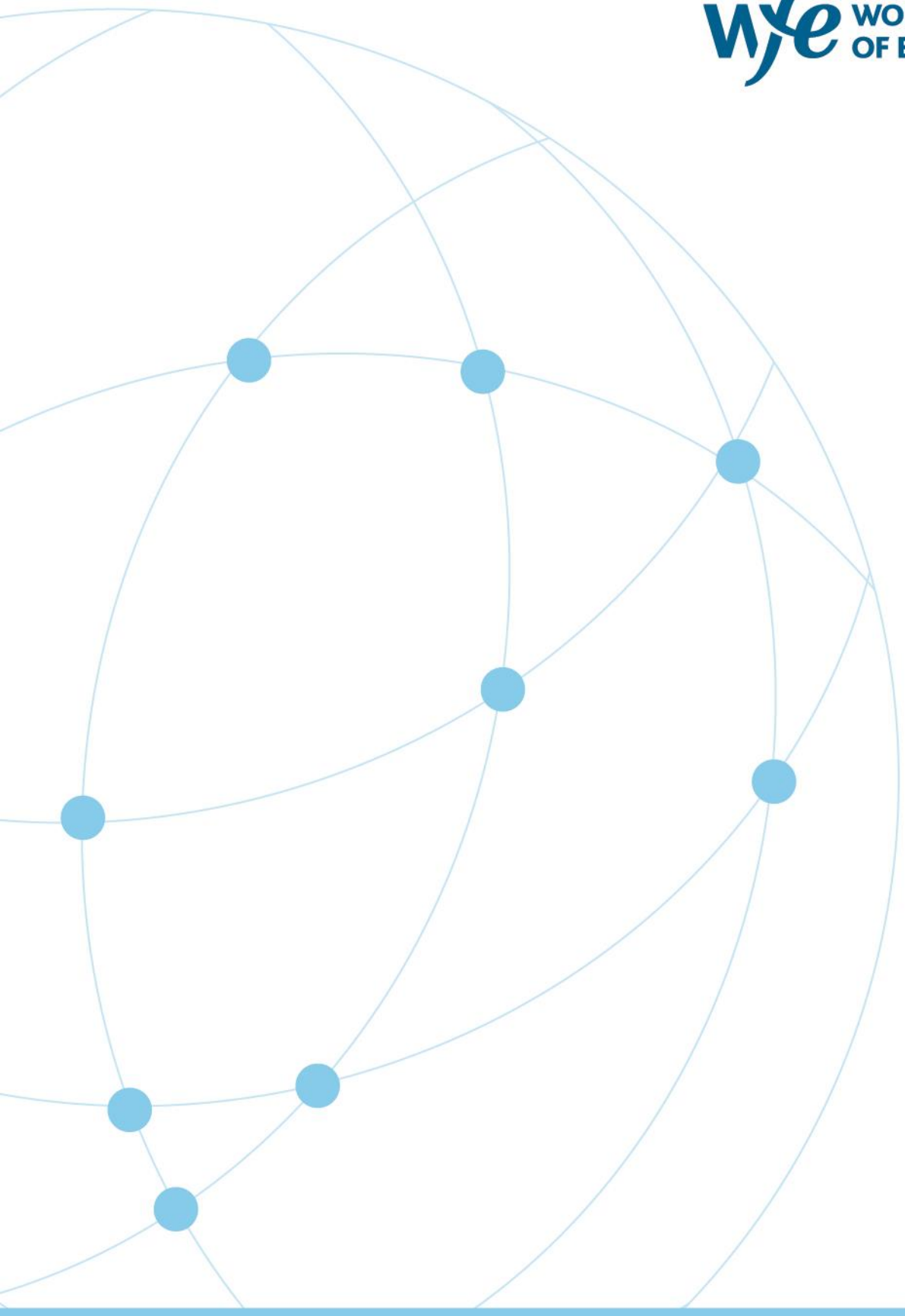

WFE Response: IOSCO Policy Recommendations for Crypto and Digital Asset Markets

31 July 2023

Background

The World Federation of Exchanges (WFE) is the global industry association for operators of regulated exchanges and clearing houses (CCPs). This includes everything from local entities in emerging markets to international groups based in major financial centres, with 34% based in Asia-Pacific, 45% in EMEA and 21% in the Americas. Collectively, they run some 250 pieces of market infrastructure, which includes standalone CCPs as well as integrated exchanges-cum-clearing houses.

As of end-2022, around $145 trillion (equivalent) in share trading annually passes through WFE members, who are home to over 55,000 listed companies, with an aggregate market capitalisation of over $100tr. WFE member's 90 CCP offerings collectively ensure that risk takers post some $1.3tr (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements.

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair and transparent environment for all sorts of companies and market participants wishing to raise capital, invest, trade, and manage financial risk.

Established in 1961 and headquartered in London, the WFE seeks outcomes that maximise financial stability, consumer confidence and economic growth. We also engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

James Auliffe, Manager, Regulatory Affairs: jauliffe@world-exchanges.org

Nicolas Höck, Junior Analyst: junior.analyst@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

or

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org.

General Comments

The World Federation of Exchanges (WFE) welcomes the opportunity to comment on this consultation. As representatives of established, regulated, and trusted exchanges we wanted to offer our views on the formation of a framework for regulating crypto-assets. Naturally, we focus on those questions that are most relevant to our membership, principally relating to trading venues and trading.

We know that technological innovation, such as that related to distributed ledgers, can enhance financial markets. DLT has the potential to deliver lower costs, faster execution of transactions, improved transparency, auditability of operations, and other benefits. Nevertheless, there have been a number of notable incidents involving the crypto-sector, with the biggest being the demise of FTX.

The recent experiences point to the need for regulation. Rather than particularly new or novel failures, the majority of issues around the crypto-sector remind us of lessons already learned in traditional finance. By supporting meaningful regulation, IOSCO can help mitigate and minimise the risk of failures. Therefore, the WFE is a strong supporter of the internationally established principles of 'same risk, same regulation.'

We also recognise that jurisdictions are at different stages of crypto regulation development. We encourage IOSCO to recommend that each jurisdiction utilise all of the tools at its disposal (e.g., rulemaking, no action letters and guidance) to help promote the ability of traditional financial market participants to support the healthy development of this evolving ecosystem.

Specific Comments

Chapter 1: Overarching Recommendation Addressed to All Regulators

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

We welcome the direction of travel that IOSCO sets out in this consultation. Basing regulations for Crypto-Asset Service Providers (CASPs) on established financial market principles like IOSCO's is a sensible proposition. Nevertheless, it should be made clear that this proposal differentiates between tokenised traditional assets and crypto-assets. The former is already regulated under the established principles and presents different risks to the latter.

This highlights one issue with IOSCO's proposed recommendations in that it does not define what a crypto-asset is. This later becomes an issue as not all crypto-assets can be treated in the same way and it becomes difficult to identify the corresponding regulation/principle to apply to a particular type of crypto-asset.

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?

We agree with IOSCO that "the regulatory approach should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets." Where possible, that should include the same risk, same rules but we recognise that the rules, at times, need to be tailored to the market specificities or adjusted where there is no exact equivalent in traditional markets.

Chapter 2: Recommendations on Governance and Disclosure of Conflicts

Question 3: – Does Chapter 2 adequately identify the potential conflicts of interest that may arise through a CASP's activities? What are other potential conflicts of interest which should be covered?

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?

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

Whether in traditional financial services (TradFi) or crypto-related markets (CeFi or DeFi), a single group or entity providing multiple functions can be an effective way of delivering services. Exchange groups in TradFi often expand their business portfolios to diversify their revenue streams and create synergies among their various subsidiaries. This diversification can help mitigate risks and stabilise their financial performance thereby helping to deliver financial stability. For example, an exchange group that owns a stock exchange and a clearinghouse can leverage the strengths of each business to enhance overall efficiency and competitiveness.

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

Nevertheless, exchange groups have robust conflict of interest management procedures to ensure ethical and fair practices. This involves implementing policies and mechanisms that prevent any undue advantage or bias among the businesses owned by the group. Transparent governance structures, independent oversight, disclosure requirements, and compliance frameworks are some of the measures that have been proven to mitigate conflicts of interest effectively. Furthermore, exchanges and other trading venues do not trade against their own clients as a protection against abuses.

IOSCO's recommendations should address this situation with regards to CASPs, following the logic that IOSCO is seeking to "achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets."

Finally, the WFE would also like to take the opportunity to highlight the importance of distinguishing between so-called "cryptoasset exchanges" and the regulated, secure and lit markets that established exchanges provide. Since the emergence and popularity of crypto-currencies, crypto-asset trading platforms have been referred to as "exchanges", implying that they qualify as such in the traditional sense. This can mislead investors into thinking that such entities are regulated or meet the regulatory standards of traditional exchanges where they are not or do not (a perception that has unfortunately been falsely perpetuated by some "crypto-asset exchanges" in the recent past). For example, traditional exchanges typically have transparency in matching algorithms or order books this is not necessarily the case with CASPs and alternative venues, especially DeFi matching protocols where queue jumping frequently occurs.

While some crypto-asset platforms are regulated, or enforce their own standards, unless they are recognised by regulatory authorities and adhere to a set of acknowledged regulations, they cannot offer the same security to market participants. This includes having an appropriate level of pre- and post-trade transparency. In this context, regulation

should ensure that there is no substantial difference between trading in fiat-based products and trading crypto-asset based products. The 'same risk, same rule' principle should apply

Chapter 3: Recommendations in Relation to Listing of Crypto-Assets and Certain primary Market Activities

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.

In the pursuit of 'same risk, same regulation' it is worth considering how things work in TradFi. In TradFi, exchanges are the primary market operators, and they are not allowed to trade against their clients. They perform several key functions. Firstly, exchanges police and vet the products that are listed on their venues. Requirements like these ensure that only high-quality products are traded on exchanges. This reassures investors of the integrity of both the exchange and the traded product.

Secondly, exchanges require and enforce disclosures. Issuers are obliged to disclose in a timely manner information that investors would require to enable them to make informed investment decisions, including events that pertain to the dynamics of a company or otherwise have the potential to affect share value. Thirdly, by virtue of these requirements exchanges are frequently the primary price forming venue for products traded on their venue. This means that there is a single price which other venues use.

Alternative venues or dark pools operate markets in a more limited way but are also not allowed to trade against their own clients. This is because regulators and governments were concerned about conflicts of interest due to its dual role. As an operator of the trading venue, the firm has a responsibility to maintain fair and transparent market conditions. However, as a trading intermediary, it may have an incentive to prioritize its own trading activities or those of its clients, potentially compromising the fair and equitable operation of the trading venue. For example:

- The firm operating the trading venue may have access to privileged information or preferential treatment, giving it an advantage over other market participants. This can create an unfair playing field, where the firm or its clients can exploit their informational advantage to the detriment of other traders.

- Dual-role firms may be tempted to engage in market manipulation or front-running activities. Market manipulation involves artificially influencing prices or trading volumes to benefit the firm's own trading positions. Front-running occurs when the firm executes orders on its trading venue ahead of its clients' orders, taking advantage of their trading intentions for personal gain.

- The firm's dual role may result in reduced transparency, as it may be motivated to withhold or selectively disclose certain information to serve its own interests. This lack of transparency can erode market confidence and hinder the ability of other participants to make informed trading decisions.

- Liquidity is a self-fulfilling mechanism (liquidity begets liquidity); there is a strong incentive for the platform operator to "show volumes to attract volumes"; thus creating artificial volumes to attract real volumes. A market making scheme should not be designed for that purpose but there is a thin line that is easily crossed if no regulator or supervisor is monitoring the nature of the market making.

We note that market makers or inter-dealer brokers that deal on exchanges or alternative venues may be trading against their own clients. However, these entities facilitate trading and provide liquidity by continuously quoting bid and ask prices for securities. They may take positions in the securities they trade to manage their risk or to maintain a balanced inventory and can therefore trade against their own clients. Nevertheless, they are required to disclose the fact that they may be trading against their own clients. The relevant point is that an exchange operator should not also operate a risk-taking market-making operation.

We also acknowledge that in traditional finance there are off-exchange venues operated by firms that allow the investment firm or broker-dealer operator to trade proprietarily against clients (e.g., systematic internalisers and single dealer platforms); however, these platforms are less regulated and less transparent than traditional exchanges and do not perform the primary market functions typical of exchanges. In addition, unlike the opaque arrangements of many crypto markets, clients of a systematic internalisers are aware that they are interacting with a bilateral, proprietary capital trading facility, rather than an exchange.

In crypto markets, whether CeFI or DeFi, the distinction between 'exchanges,' dark pools and market makers/dealer brokers is murky. The typical business model of a crypto-trading platform (CTP) is one where the Platform serves as (i) a venue of exchange, operating the platform on which buyers and sellers trade virtual and fiat currencies; (ii) in a role similar to a traditional broker-dealer, representing traders and executing trades on their behalf; (iii) as a money-transmitter, transferring virtual and fiat currency and converting it from one form to another; (iv) as owners of large virtual currency holdings; (v) as issuers of a virtual currency listed on their own and other platforms, with a direct stake in its performance and also (vi) as custodians of customer assets. This integrated approach amalgamates the roles typically distinct in TradFi and is characteristic of CeFi/DeFi platforms.

Following the logic that IOSCO is seeking to "achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets," at the very least, IOSCO should seek to apply the same strict rules and safeguards on firms operating trading venues while also acting as trading intermediaries, such as:

- Strong, clear and simple disclosure requirements. If CTP calls itself an "exchange" or offer multilateral trading, it should be clear and unambiguous that the platform does not trade against its own clients.
- Segregation of activities between the trading platform and other functions, possibly including requiring a separate legal entity with distinct management and operational teams, physical separation of activities and segregated execution systems. These are similar requirements placed onto investment firms that wish to trade on their affiliated dark pool and/or Systematic Internalizer.
- Requiring CTPs to execute client orders in a manner that achieves the most favourable terms reasonably available under the prevailing market conditions (i.e., best execution requirements). As there is no such thing as a primary exchange for any given crypto-asset, there is frequent price difference across CASPs and consumers may not be getting the best price. An intermediary in the crypto world who also operates a trading platform may be tempted to direct all trades to their platform but this would likely be a poor outcome for its clients.
- Finally, as explained in the answer to questions 3-5. These firms should not be able to trade against their own clients. This is a firmly established principle in traditional financial services.

As part of the above suggestions, regulators ought to consider carefully whether an actor should obtain a separate license for whatever the activity is they are performing.

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?

Conducting transactions "off-chain" can offer significant benefits. The trading platform can benefit from costs-savings related to gas fees as well as increased internal efficiencies. However, IOSCO rightly notes that there is a risk of a loss of transparency in the market.

Therefore, CASPs could be required to report in similar ways to exchanges and alternative venues in TradFi. For example, pre-trade it is generally accepted that trading venue operators in TradFi must make public, on a continuous basis during normal trading hours, current bid and offer prices and the depth of trading interest at the prices advertised. Post-trade rules generally require the price, volume and time of transactions executed on the trading venue as close to real-time as technically possible.

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

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 welcome the proposed recommendations on listings. We have long called for minimum requirements for listings as we consider that these requirements help build trust in exchange listed products.

As explained in the answer to questions 3-5, it is not appropriate for CASPs to trade against their own clients. Similarly, it is not appropriate for CASPs to favour its own crypto-assets over others as that may artificially inflate the price.

Chapter 6: Recommendation on Cross-Border Cooperation

Question 13. Which measures, or combination of measures, would be the most effective in supporting cross-border cooperation amongst authorities? What other measures should be considered that can strengthen cross-border co-operation?

Harmonisation and reliance on mutual standards would be effective in supporting cross-border co-operation and managing cross-border trade (which is occurring regardless of the co-operation). When regulatory frameworks are harmonised, regulatory authorities can have a common understanding of the requirements and expectations for market participants. This consistency simplifies cross-border transactions and enhances cooperation by reducing regulatory complexity and confusion.

Moreover, when standards and regulations are aligned, it becomes easier to exchange information and communicate effectively. Regulatory authorities can collaborate on areas such as risk assessment, supervisory practices, and enforcement actions, enabling them to make better-informed decisions and coordinate their efforts. When regulatory authorities share common expectations and collaborate on enforcement actions, it becomes more challenging for market participants to exploit regulatory arbitrage or engage in fraudulent activities across borders. This promotes confidence in cross-border transactions and fosters a level playing field for market participants.

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

IOSCO's work here is an excellent starting point for harmonisation and co-operation. However, without mutually agreeing definitions for crypto-assets it will be difficult to encourage co-operation.

Chapter 7: Recommendations on Custody of Client Monies and Assets

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

In any custody arrangement for digital assets, the security of the private key holds high importance. Critical decisions must be made regarding the storage format, environment, and the procedures and timelines involved in utilising the private key for transaction authentication. In general, there are three options for storing the key: (a) "self-custody" or a "non-custodial" arrangement, where the client retains control over the key (b) a "custodial" arrangement, where a custodian securely stores the key on behalf of the client; or, (c) a hybrid of the two.

The wide array of available services and solutions in the market has a direct impact on the legal ownership and risk assessment that clients must undertake. It is important to recognise that these analyses will vary in each case, as there is no universally applicable approach. Solutions that provide clients with the private key, known as self-custody or non-custodial wallet solutions, may not fulfil the rigorous financial crime protection, security, and deployment requirements of sophisticated institutional clients in the present landscape. Moreover, these self-custody solutions may be inappropriate for unsophisticated investors.

We strongly recommend IOSCO consider whether an actor should obtain a separate license when offering self-custody services. A separate license offers further legal protections to end users which could be beneficial in case of any insolvency issues.

Finally, IOSCO could refer to the Digital Assets Custody Standard defined by CMTA (Digital Assets Custody Standard — CMTA, The Capital Markets and Technology Association) as a guideline on how to store crypto assets

Question 15. (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?

When dealing with rapidly developing technologies, regulation ought to be principles-based. This ensures tech neutrality and enables innovative business models to emerge.

Question 15. (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?

It is crucial to have a clear segregation between the custodian and the market infrastructure they engage with. This separation reduces the risk of investor harm should the market infrastructure find itself in trouble. When assets are held by a single entity that also offers pricing and execution services, and that entity assumes market risk, any failure in its liquidity or risk management can result in severe consequences for those who have entrusted their assets to that provider. Therefore, having an independent third-party custodian or custodian that is a separate legal entity that is solely focused on safeguarding assets without taking on liquidity or market risks is an important safeguard for clients.

Furthermore, when clients rely on a third-party for custody services, it is important for them to comprehend both the technological solution employed by the provider and the legal framework that governs the storage and usage of the encryption key, as well as the digital assets controlled by that key. If the digital asset custodian misapplies the appropriate characterisation, clients face the risk of losing control over their private keys and potentially sacrificing access to the digital assets associated with those keys.

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

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

In such situations, customers rely on the terms set forth by the digital asset custodian and, to a certain extent, the custodian's willingness to compensate for the stolen assets. It is important to note that, in general, there is no regulatory requirement for the custodian to fully reimburse the customer in such circumstances. While specific legal principles may apply in certain jurisdictions, their applicability in the context of digital assets may not be straightforward. The year 2021 witnessed digital asset-related scams resulting in the loss of over $6.2 billion[1] worth of digital assets, underscoring the magnitude of this issue and highlighting the market potential for digital asset custodians that prioritize top-tier security measures.

[1] See FT: The Lawless World of Crypto Scams

Chapter 8: Recommendation to Address Operational and Technological Risks

Question 17. Are there additional or unique technology/cyber/operational risks related to crypto-assets and the use of DLT which CASPs should take into account? If so, please explain.

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

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

For private DLT (like tokenised traditional securities), the risks are substantially the same. This is because the DLT is controlled by a single entity that can fix errors in the system. For public DLT (like Bitcoin and Ethereum) no one entity can step in and fix errors in the system. So, for example, when in 2016 Ethereum was compromised in the DAO attack, in which an unsecure DAO contract was hacked and over 3.6 million ETH (60 million USD) were stolen, there was no immediate recourse to return these funds.

Instead, 85% of the Ethereum community voted to implement a hard fork. The DAO's ether was transferred to a separate smart contract during the hard fork, allowing investors to withdraw their money and effectively rolling back the Ethereum network's history to before the DAO hack. Since blockchains are meant to be immutable and censorship-resistant, this was incredibly contentious and has never occurred again, at least for Ethereum.

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

Chapter 10: Box Text on Stablecoins

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

Many so-called stablecoins operate similarly to Money Market Funds (MMFs). Although MMFs are highly liquid and often considered as "cash equivalents;" units in an MMF are not used as a medium of exchange or a unit of account. Therefore, MMFs are not used as currency like stablecoins.

The reason that MMFs are not used as currency are clear. Redemption risks have been observed with MMFs during significant market events, such as the 2008/2009 financial crisis and the early stages of the COVID-19 pandemic. If a stablecoin were to face a substantial volume of redemption requests, it could encounter difficulties in fulfilling those requests promptly and is therefore not stable enough to be a currency.

While stablecoins frequently emphasise transparency and may provide attestations from independent third parties, the level of transparency they offer is often insufficient. Merely disclosing the amount of cash and assets held by a stablecoin is not comprehensive enough to ensure transparency. Disclosures should be more detailed and in-depth.

This is particularly important as stablecoins often invest in cryptocurrencies, which introduces a pro-cyclicality risk. In the event of a decline in the value of cryptocurrencies like Bitcoin, investors may sell off their holdings. This increased

selling pressure on the stablecoin can further drive down the price of the cryptocurrency. Consequently, the stablecoin may struggle to maintain its peg to the underlying currency.