

# **Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms**

## **Consultation Report**



**OICU-IOSCO**

**BOARD OF THE  
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS**

**CR02/2019**

**MAY 2019**

This paper is for public consultation purposes only. It has not been approved for any other purpose by the IOSCO Board or any of its members.

Copies of publications are available from:  
The International Organization of Securities Commissions website [www.iosco.org](http://www.iosco.org)

© *International Organization of Securities Commissions 2019. All rights reserved. Brief excerpts may be reproduced or translated provided the source is stated.*

## Foreword

The Board of the International Organization of Securities Commissions (IOSCO) has published this Consultation Report on Crypto-Asset Trading Platforms to encourage the public to comment on the identified issues, risks, key considerations and related toolkits.

## How to Submit Comments

Comments may be submitted by one of the three following methods **on or before 29 July 2019**. To help us process and review your comments more efficiently, please use only one method.

**Important:** All comments will be made available publicly, unless anonymity is specifically requested. Comments will be converted to PDF format and posted on the IOSCO website. Personal identifying information will not be edited from submissions.

### 1. Email

- Send comments to [consultation-02-2019@iosco.org](mailto:consultation-02-2019@iosco.org)
- The subject line of your message must indicate 'Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms.'
- If you attach a document, indicate the software used (e.g., WordPerfect, Microsoft WORD, ASCII text, etc.) to create the attachment.
- Do not submit attachments as HTML, PDF, GIFG, TIFF, PIF, ZIP or EXE files.

### 2. Facsimile Transmission

Send by facsimile transmission using the following fax number: + 34 (91) 555 93 68.

### 3. Paper

Send 3 copies of your paper comment letter to:

Giles Ward  
International Organization of Securities Commissions (IOSCO)  
Calle Oquendo 12  
28006 Madrid  
Spain

Your comment letter should indicate prominently that it is a "*Public Comment on Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms.*"

## Contents

<b>Chapter</b>	<b>Page</b>
<b>1. Executive summary</b>	<b>1</b>
<b>2. Introduction</b>	<b>3</b>
<b>3. Regulatory Approaches to Crypto-Asset Trading Platforms</b>	<b>6</b>
<b>4. Key Considerations</b>	<b>10</b>
<b>5. Cross Border Information Sharing</b>	<b>26</b>
<b>6. Conclusion</b>	<b>28</b>
<b>Annex A</b>	<b>29</b>
<b>Annex B</b>	<b>35</b>

## Chapter 1 - Executive Summary

The emergence of crypto-assets is an important area of interest for regulatory authorities, including those with authority over secondary markets and the trading platforms that facilitate the secondary trading of crypto-assets (Crypto-Asset Trading Platforms or CTPs). The aim of this Consultation Report is to assist IOSCO members in evaluating the issues and risks relating to CTPs.

Published in February 2017, the *IOSCO Research Report on Financial Technologies (Fintech)*,<sup>1</sup> (the Fintech Report) discussed distributed ledger technologies (DLT) and the role of tokenization of assets and fiat money. In the Fintech Report, IOSCO noted that “Tokenization is the process of digitally representing an asset, or ownership of an asset. A token represents an asset or ownership of an asset. Such assets can be currencies, commodities or securities or properties.” For this Consultation Report, crypto-assets are a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, and can represent an asset such as a currency, commodity or security, or be a derivative on a commodity.

Where a regulatory authority has determined that a crypto-asset or an activity involving a crypto-asset falls within its jurisdiction, IOSCO’s Objectives and Principles of Securities Regulation<sup>2</sup> (IOSCO Principles) and the Assessment Methodology<sup>3</sup> (the Methodology) provide useful guidance in considering the novel and unique issues and risks that arise in this new market. The IOSCO Principles and Methodology also facilitate the promotion of IOSCO’s core objectives of securities regulation<sup>4</sup>, which include protecting investors and ensuring that the markets are fair, efficient and transparent.

The Consultation Report, prepared by Committee 2 on the Regulation of Secondary Markets (Committee 2)<sup>5</sup>, is based in part on the information gathered by Committee 2 related to the operation of CTPs and the regulatory approaches that are currently applied or are being considered in Committee 2 member jurisdictions or in member jurisdictions that participate in IOSCO’s ICO Consultation Network (ICO Network).<sup>6</sup>

---

<sup>1</sup> <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf>

<sup>2</sup> Published at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf>

<sup>3</sup> Published at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD562.pdf>

<sup>4</sup> In the IOSCO Principles and Methodology, the words “securities markets” are used, where the context permits, to refer compendiously to the various market sectors. In particular, where the context permits, they should be understood to include reference to the derivatives markets. The same applies to the use of the words “securities regulation”. (See *IOSCO By-Laws, Explanatory Memorandum*).

<sup>5</sup> Chaired by Ontario, C2 members include representatives of regulatory authorities from: Australia, Brazil, Canada (OSC, AMF Quebec, IIROC), China, Dubai, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Republic of Korea, Kuwait, Malaysia, Mexico, The Netherlands, Nigeria, Romania, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States of America (CFTC, SEC).

<sup>6</sup> The ICO Network was established by IOSCO in January 2018 and facilitates sharing experiences and concerns with fellow regulators. Jurisdictions in the ICO Network that are not in Committee 2 are: Argentina, Abu Dhabi, the Bahamas, Belgium, Canada (Alberta, British Columbia), Chile, Gibraltar, European Union (ESMA), Isle of Man, Israel, Jersey, Liechtenstein, New Zealand, Poland, Serbia, Thailand, Trinidad and Tobago and the United States (FINRA).

The Consultation Report describes issues and risks identified to date that are associated with the trading of crypto-assets on CTPs. In relation to the issues and risks identified, it describes key considerations and provides related toolkits that are useful for each key consideration. These key considerations and toolkits are intended to assist regulatory authorities who may be evaluating CTPs within the context of their regulatory frameworks.<sup>7</sup> The key considerations relate to:

- Access to CTPs;
- Safeguarding participant assets;
- Conflicts of interest;
- Operations of CTPs;
- Market integrity;
- Price discovery; and
- Technology.

The operational model adopted by a CTP and the existing regulatory framework may determine the extent to which issues or risks exist, are relevant or have already been mitigated. IOSCO recognizes that this market is new and rapidly evolving. As a result, the key considerations and toolkits put forward in the Consultation Report are not intended to suggest or mandate any particular regulatory action or requirement. They represent specific areas that IOSCO believes jurisdictions could consider in the context of the regulation of CTPs.

The toolkits are examples of measures that can be used by regulatory authorities to address the key considerations and the associated risks and issues. For any particular IOSCO member there may be other considerations not highlighted in this report that it views as relevant to its legal and regulatory framework. IOSCO will continue to monitor the evolution of the markets for crypto-assets, with a view to ensuring that the issues, risks and key considerations identified in this report remain relevant and appropriate.

Finally, this Consultation Report does not include an analysis of the criteria that is used by regulatory authorities to determine whether a crypto-asset falls within its remit. Rather, it focuses on the trading of crypto-assets on CTPs when the regulatory authority has determined that it has the legal authority to regulate those assets or the specific activity involving those assets.

---

<sup>7</sup> In some jurisdictions, the existing regulatory framework for the trading of derivatives on exchanges may apply to the trading of crypto-asset derivatives (e.g., United States). Consideration of such frameworks may entail a separate review from those contemplated in this Consultation Report.

## Chapter 2 – Introduction

### 1. Background

For this Consultation Report, crypto-assets are a type of private asset that depends primarily on cryptography and DLT<sup>8</sup> or similar technology, as part of its perceived, or inherent value.<sup>9</sup> Crypto-assets can represent an asset or ownership of an asset, such as a currency, commodity, security, or derivative on a commodity.

Regulatory authorities globally are examining the issues surrounding crypto-asset trading, including whether these assets are securities or other financial instruments, whether they fall within their regulatory jurisdiction, and, if so, how to address the novel and unique issues and risks that may be associated with these assets and the CTPs where they trade.

The G20 Ministers of Finance and Central Bank Governors acknowledged in the Communiqué following their March 2018 meeting in Buenos Aires that crypto-assets are not a material risk to financial stability, but stated that they “raise issues with respect to consumer and investor protection, market integrity, tax evasion, money laundering and terrorist financing”.<sup>10</sup> They called on international standard setting bodies “to continue their monitoring of crypto-assets and their risks, according to their respective mandates, and assess multilateral responses as needed.”<sup>11</sup>

IOSCO members have raised concerns about crypto-assets in areas ranging from trading, custody, clearing and settlement, accounting, valuation, and intermediation, to the exposure of investment funds to crypto-assets. In January 2018, IOSCO issued a statement on concerns related to Initial Coin Offerings (ICOs),<sup>12</sup> noting that there are clear risks associated with ICOs, including the targeting of retail investors through online distribution channels by parties often located outside of an investor’s home jurisdiction. IOSCO also announced the establishment of the ICO Network<sup>13</sup> through which IOSCO members could discuss and share their experiences and concerns with fellow regulators.

Committee 2 began examining issues relating to secondary market trading of crypto-assets on CTPs in early 2018. Initially, Committee 2 identified several issues that could be considered by regulatory authorities, including: (1) transparency; (2) custody, clearing and settlement; (3) trading; and (4) cyber security and systems integrity. Committee 2 has continued its work since May 2018 and, in October 2018, the IOSCO Board supported Committee 2 in the development of this Consultation Report.

---

<sup>8</sup> The October 2018 FSB report *Crypto-asset markets: Potential channels for future financial stability implications* defines DLT as a means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations. Available at:

<http://www.fsb.org/wp-content/uploads/P101018.pdf>.

<sup>9</sup> Ibid.

<sup>10</sup> [https://back-g20.argentina.gob.ar/sites/default/files/communique\\_-\\_finance\\_and\\_central\\_banks\\_-\\_march\\_2018.pdf](https://back-g20.argentina.gob.ar/sites/default/files/communique_-_finance_and_central_banks_-_march_2018.pdf).

<sup>11</sup> Ibid.

<sup>12</sup> <https://www.iosco.org/news/pdf/IOSCONEWS485.pdf>.

<sup>13</sup> See supra note 7.

In building on previous work and preparing this Consultation Report, Committee 2 relied on information received in response to a survey (the Survey) sent to its member jurisdictions and participants in the ICO Network. The Survey requested details about the types of CTPs that are operating (not necessarily licensed or authorized) and how CTPs are accessed by participants. The Survey also sought comment on the identification of associated risks or issues by regulatory authorities, and what regulatory approaches were in place, or being contemplated to address any concerns. IOSCO and other international bodies, along with national regulatory authorities, continue to monitor the growth and development of crypto-assets, including the trading of such assets on CTPs and other areas relevant to the global financial markets.<sup>14</sup>

## 2. Scope

For this Consultation Report, a Crypto-Asset Trading Platform is defined as a facility or system that brings together multiple buyers and sellers of crypto-assets for the purpose of completing transactions or trades. While CTPs perform functions that are similar to Trading Venues,<sup>15</sup> they may also perform functions that are more typically performed by intermediaries, custodians, transfer agents and clearing houses.

The Consultation Report focuses on the approaches taken or being considered by regulatory authorities in Committee 2 member jurisdictions and jurisdictions in the ICO Network, where the regulatory authority has determined that it has legal authority to regulate crypto-assets and/or instruments based on, or specific activities involving, crypto-assets. For example, in some jurisdictions, legal authority is based on the classification of the crypto-asset as a security, a financial instrument, an asset, a commodity or a derivative.<sup>16</sup>

The Consultation Report focuses on the issues and risks related to CTPs that have been identified to date. The Consultation Report does not include an analysis of the criteria that is used by regulatory authorities to determine whether a crypto-asset falls within its remit. Finally, the Consultation Report focuses on secondary market trading of crypto-assets on CTPs and it does not discuss issues related to initial coin offerings (ICOs).

## 3. Purpose

IOSCO believes that fostering innovation should be balanced with the appropriate level of regulatory oversight. Accordingly, while aspects of the underlying technology and operation of CTPs may be novel, if a CTP trades a crypto-asset that is a security and it falls within a regulatory authority's jurisdiction, the basic principles or objectives of securities regulation

---

<sup>14</sup> *Board Priorities – IOSCO Work Program for 2019*. See: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD625.pdf>

<sup>15</sup> In this Consultation Report, the term Trading Venue refers to traditional exchanges, alternative trading systems (ATSS), multilateral trading facilities (MTFs) or other regulated trading venues. We recognize, however, that the concept of a “trading venue” is evolving in a number of Committee 2 jurisdictions. For example, the concept may, at the discretion of individual members for their jurisdictions, also include swap execution facilities (SEFs) in the United States or organized trading facilities (OTFs) in the European Union.

<sup>16</sup> Depending on jurisdictional authority, the scope of this Consultation Report could be useful to a variety of CTPs that trade different types of crypto-assets.



(investor protection, ensuring fair, efficient and transparent markets and investor confidence in markets) should apply.

Based on the findings of the Survey and prior Committee 2 work, the Consultation Report highlights some of the unique issues associated with CTPs and provides key considerations to assist regulatory authorities. The key considerations, issues and risks identified in the Consultation Report may not always be relevant and may currently be mitigated or addressed by existing regulatory frameworks. IOSCO believes they are important areas for regulatory authorities to consider in the context of the regulation of CTPs. The Consultation Report also references the relevant IOSCO Principles and the Methodology that are useful for analyzing the potential issues and risks identified. The IOSCO Principles are the overarching core principles for securities regulation that guide IOSCO in the development and implementation of internationally recognized and consistent standards of regulation, oversight and enforcement.

IOSCO recognizes the evolving nature of crypto-asset markets globally, including in emerging market jurisdictions. As a result, it is not possible or appropriate to provide a definitive list of the risks, issues and outcomes at this time, nor is it appropriate to prescribe new standards or requirements. However, IOSCO believes that it is useful to outline the issues and risks identified to date, highlight key considerations, reference the IOSCO Principles and provide toolkits that can be used by regulatory authorities to address the underlying issues or risks associated with each key consideration. As noted above, these key considerations are not intended to be a mandatory set of standards or requirements that jurisdictions are expected to adopt in their regulation of CTPs. Similarly, not every item in the toolkits may be relevant to every regulatory authority.

Over time, IOSCO intends to continue to monitor the evolution of this market and review and update this report, if necessary.

## Chapter 3 - Regulatory Approaches to Crypto-Asset Trading Platforms

Many of the issues and risks associated with trading on CTPs are similar to the issues and risks associated with trading traditional securities or other financial instruments on Trading Venues. Consequently, IOSCO's three core objectives of securities regulation are relevant: (1) the protection of investors; (2) ensuring that markets are fair, efficient and transparent; and (3) the reduction of systemic risk.<sup>17</sup> Supporting these objectives are principles that foster efficient markets, including: effective price discovery, appropriate transparency, market integrity and fair access.

### 1. Relevant IOSCO Principles

The IOSCO Principles set out a broad framework for the regulation of securities<sup>18</sup> and include principles specific to Trading Venues. This Consultation Report identifies some of the IOSCO Principles and the Methodology that provide useful guidance, including those relating to: (1) Cooperation, (2) Secondary and Other Markets, (3) Market Intermediaries and (4) Clearing and Settlement.

#### *(a) IOSCO Principles Relating to Cooperation*

The IOSCO Principles relating to cooperation, specifically, Principles 13, 14 and 15, address cooperation amongst regulators and their domestic and foreign counterparts for, among other regulatory purposes, investigations, supervision and enforcement. While not unique to CTPs, these principles are important for regulatory authorities to consider in this context as CTPs tend to operate across multiple jurisdictions. These principles are:

- IOSCO Principle 13 - The Regulator should have authority to share both public and non-public information with domestic and foreign counterparts.
- IOSCO Principle 14 - Regulators should establish information sharing mechanisms that set out when and how they will share both public and non-public information with their domestic and foreign counterparts.
- IOSCO Principle 15 - The regulatory system should allow for assistance to be provided to foreign Regulators who need to make inquiries in the discharge of their functions and exercise of their powers.

#### *(b) IOSCO Principles for Secondary and Other Markets*

The IOSCO Principles for Secondary and Other Markets are set out in Principles 33 through 37. These are:

- IOSCO Principle 33 - The establishment of trading systems including securities exchanges should be subject to regulatory authorization and oversight.
- IOSCO Principle 34 - There should be ongoing regulatory supervision of exchanges and trading systems which should aim to ensure that the integrity of trading is

---

<sup>17</sup> While the reduction of systemic risk is one of IOSCO's core objectives, it is not addressed in this Consultation Report. In July 2018, the FSB agreed that crypto-assets do not pose a material risk to global financial stability issue at this time. *See:* <http://www.fsb.org/wp-content/uploads/P160718-1.pdf>

<sup>18</sup> Methodology, Page 13.

maintained through fair and equitable rules that strike an appropriate balance between the demands of different market participants.

- IOSCO Principle 35 - Regulation should promote transparency of trading.
- IOSCO Principle 36 - Regulation should be designed to detect and deter manipulation and other unfair trading practices.
- IOSCO Principle 37 – Regulation should aim to ensure the proper management of large exposures, default risk and market disruption.<sup>19</sup>

*(c) IOSCO Principles Relating to Market Intermediaries and Principles Relating to Clearing and Settlement*

Some CTPs may perform functions that are not typically performed by Trading Venues and are more similar to functions performed by intermediaries (e.g., on-boarding retail investors or providing custody of assets). For these CTPs, the IOSCO Principles for Market Intermediaries provide useful guidance to regulatory authorities who are considering CTP issues. They include:

- IOSCO Principle 29 – There should be minimum entry standards for market intermediaries.
- IOSCO Principle 30 - There should be initial and ongoing capital and other prudential requirements for market intermediaries that reflect the risks that the intermediaries undertake.
- IOSCO Principle 31 - Market intermediaries should be required to establish an internal function that delivers compliance with standards for internal organization and operational conduct, with the aim of protecting the interests of investors and their assets and ensuring proper management of risk, through which management of the intermediary accepts primary responsibility for these matters.
- IOSCO Principle 32 - There should be procedures for dealing with the failure of a market intermediary in order to minimize damage and loss to investors and to contain systemic risk.<sup>20</sup>

Depending on the arrangements for clearing and settlement by the CTP, IOSCO Principle 38 also provides useful guidance to regulatory authorities who are considering CTP issues. It states:

- IOSCO Principle 38 - Securities settlement systems and central parties should be subject to regulatory and supervisory requirements that are designed to ensure that they are fair, effective and efficient and that they reduce systemic risk.<sup>21</sup>

The Methodology for each IOSCO Principle details the Key Issues and Key Questions relevant to that Principle and provides useful guidance to regulatory authorities considering the wide range of issues raised by CTPs and the appropriate regulatory approach for their jurisdiction.

---

<sup>19</sup> Consideration of elements of Principle 37 that relate to systemic risk are excluded from this Consultation Report. We identify Principle 37 as relevant in the context of market integrity.

<sup>20</sup> Consideration of elements of Principle 32 that relate to systemic risk are excluded from this Consultation Report. We identify Principle 32 as relevant in the context of investor protection.

<sup>21</sup> Consideration of elements of Principle 38 that relate to systemic risk are excluded from this Consultation Report. We identify Principle 38 as relevant in the context of ensuring that markets are fair, effective and efficient.

## 2. Regulatory Approaches

Committee 2 received thirty-four responses to the Survey.<sup>22</sup> The responses outlined some of the CTP models that are operational (but not necessarily licensed or authorized by regulatory authorities), described the risks and issues identified by regulatory authorities, and how such risks and issues have been, or could be addressed (i.e., the existing, adopted regulatory framework or regulatory responses that are under consideration).

The Survey responses demonstrate that the approaches to the regulation of CTPs differ among jurisdictions. For example:

- The majority of respondents apply their existing regulatory frameworks to CTPs when the crypto-assets traded qualify as securities or other financial instruments.
- A number of jurisdictions have established, or are in the process of establishing, a specific framework for CTPs that offer trading of crypto-assets that fall within their regulatory remit. Some jurisdictions are creating a new regime or adapting the existing one by tailoring requirements and/or exemptions. In some jurisdictions, the payment service framework applies.
- Some respondents indicated that the existing regulatory framework does not apply to CTPs, primarily because crypto-assets are not financial instruments as defined in existing rules.
- In some jurisdictions, the trading of crypto-assets is banned.

The Survey responses also highlight different approaches to address the same issues and risks related to CTPs, including those related to the:

- Access to, and on-boarding of investors;
- Safekeeping of participant assets, including custody arrangements;
- Identification and management of conflicts of interest;
- Transparency of operations;
- Market integrity, including the rules governing trading on the CTP and how those rules are monitored and enforced;
- Price discovery mechanisms;
- Technology, including resiliency and cyber security;
- Clearing and settlement; and
- Cross-border information sharing and regulatory cooperation.

Finally, in response to the Survey, many IOSCO members provided information with respect to the regulatory framework applicable to CTPs that are within their jurisdiction (see Annex A of this Consultation Report for list of relevant publications). A more detailed discussion of the key findings from the Survey can be found at Annex B.

---

<sup>22</sup> Responding jurisdictions are: Abu Dhabi, Argentina, Australia, Brazil, British Columbia, Chinese Mainland, Dubai, France, Germany, Gibraltar, Hong Kong, Ireland, Italy, Japan, Jersey, Kuwait, Malaysia, Mexico, Netherlands, New Zealand, Ontario (OSC and IIROC), Quebec, Romania, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom, United States (CFTC and SEC).

Based on the Survey responses, it is clear that since many CTPs perform functions that are not typically performed by Trading Venues, an analysis of CTP operational models is important. The following initial questions may aid this analysis and inform decisions related to appropriate regulatory approaches.

- Who can access the CTP?
- How does the trading system operate, and what are the rules of that system?
- Which crypto-assets are eligible for trading?
- How are crypto-assets priced on the CTP?
- What degree of transparency of trading is provided?
- How does the CTP seek to prevent market abuse?
- What clearance and settlement processes exist?
- How are participant assets held?
- What possible conflicts of interest exist?
- What cyber security and system resiliency controls are in place?

Each of these questions relate to key issues and risks that may impact investors and fair, efficient and transparent markets. The section below describes the key considerations and the relevant IOSCO Principles and provides toolkits that can be used to address the underlying issues and risks associated with each key consideration.

## Chapter 4 - Key Considerations

Many of the issues and risks associated with trading on CTPs are similar to those associated with trading on Trading Venues. However, because of the operational models of some CTPs, unique issues and risks arise, and may prompt regulatory authorities to consider new, alternative or tailored regulatory approaches, to the extent permissible by law.

### 1. Access to Crypto-Asset Trading Platforms

*A key consideration for regulatory authorities is how access is provided to CTPs. If CTPs provide non-intermediated access to investors, another key consideration is who is responsible for the on-boarding process and how it is being performed.*

Understanding the criteria for accessing a CTP and the participant on-boarding process is important from a regulatory perspective. First, the access criteria and the on-boarding process may support a “gatekeeping” role that assists in preventing criminal or illegal trading activity on a CTP (e.g., money laundering). The access criteria may also protect investors by limiting participation on the CTP to eligible participants and, if applicable, participants with specific risk tolerance levels.

Access criteria differ between CTPs. Some restrict trading access to regulated intermediaries, others provide non-intermediated access to institutions and some CTPs provide non-intermediated access to retail investors. The latter approach is novel to CTPs as Trading Venues that provide non-intermediated access rarely provide such access to retail investors.

#### *(a) Access Criteria*

The Methodology for IOSCO Principle 33 describes considerations related to access to a system or exchange and provides useful guidance for the regulation of CTPs. In particular, Key Issue 4(b) of IOSCO Principle 33 states that the market and/or the regulator should:

*Ensure that access to the system or exchange and to associated products is fair, transparent and objective, and consider the related admission criteria and procedures.*

The Methodology emphasizes the need to articulate who can access the system or exchange and apply the criteria fairly and on a non-discriminatory basis. Transparency of the criteria enables participants and regulatory authorities to determine how access is granted or denied (both the decision process and the mechanisms for enforcing these decisions), how access is suspended or terminated and whether there are any restrictions on, or differences in access and trading. If a CTP provides non-intermediated access to retail investors, regulatory authorities may consider if there is a need to enhance fairness and transparency.

#### *(b) Participant On-boarding*

As previously noted, it is typically intermediaries that access Trading Venues on behalf of their clients (i.e., investors). Intermediaries are usually responsible for the process of investor on-boarding, which includes complying with know-your-client requirements (KYC), anti-money

laundering requirements/countering of the financing of terrorism (AML/CFT) and conducting suitability assessments (i.e., determining whether a product is appropriate for a particular client). However, where investors, particularly retail investors, have non-intermediated access to a CTP, an important consideration for regulatory authorities is who is performing the on-boarding process.

In some CTP models, the CTP may perform the on-boarding functions that would otherwise be performed by an intermediary. Where the on-boarding processes used by CTPs are limited or opaque, there may be a risk of the platform being used for illegal activities. This risk may be enhanced, for example, where the technology provides the ability to: (1) transfer funds anonymously between parties, and (2) mask the origin or destination of the flow of funds. In addition, there may be regulatory arbitrage if investors are permitted to access a CTP from jurisdictions where such activities are prohibited. Finally, a CTP performing such functions may allow participants, particularly retail investors, to be on-boarded when the trading of crypto-assets is not suitable for them, and may create a risk of investor harm.

Where CTPs on-board participants, including retail investors, the Key Issues of IOSCO Principle 31 provide useful guidance to evaluate the issues and risks. For example, Key Issue 11(a) of Principle 31 sets out an important component relating to a market intermediary's conduct with clients:

*When establishing a business relationship with a client, a market intermediary should identify, and verify, the client's identity using reliable, independent data. A market intermediary should also obtain sufficient information to identify persons who beneficially own or control securities and, where relevant, other accounts. Procedures to implement this requirement will facilitate a market intermediary's ability to mitigate the risk of being implicated in fraud, money laundering, or terrorist financing.*

Regardless of whether they facilitate trading in crypto-assets that are securities, some CTPs may already be subject to AML/CFT legislation. In some other jurisdictions, legislation has either been passed or is being considered that would subject CTPs to such requirements. In addition, the Financial Action Task Force (FATF) has recognized the need to address risks in this area and is engaged in ongoing work applying the FATF standards to “virtual assets” and “virtual asset service providers”.<sup>23</sup>

Where retail investors are permitted to have direct access to CTPs, a consideration of whether CTPs are undertaking any investor suitability assessments prior to account opening is important. Such on-boarding assessments are an important element of investor protection to ensure that investors are participating in asset classes that match their individual financial situations/risk tolerances and to mitigate risks of significant loss. Further, a consideration of whether CTPs are providing risk disclosures to investors that set out the risks of trading the types of products that may be available on a CTP are also important.

---

<sup>23</sup> In October 2018, the FATF clarified that its recommendations apply in the case of financial activities involving virtual assets. The amended Recommendation 15 requires that virtual asset service providers are regulated for AML/CFT purposes, licenced or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF recommendations. In February 2019, the FATF published for comment more detailed implementation requirements for effective regulation and supervision/monitoring of virtual asset service providers in Interpretive Note to Recommendation 15. *See*: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html>)

Guidance regarding disclosure can be found in Key Issue 11(e) of IOSCO Principle 31. It emphasizes the importance of the disclosure of information to assist investors in making informed decisions. It states, in part, that:

*A market intermediary should disclose or make available adequate information to its client in a comprehensible and timely way so that the client can make an informed investment decision. It may be necessary for regulation to require a particular form of disclosure where products carry risk that may not be readily apparent to the retail client.*

## **Toolkit**

If a regulatory authority is considering the issues and risks relating to participant access to CTPs and the on-boarding process, an assessment may include:

- A review of the CTPs' policies and procedures regarding access criteria;
- Consideration of allowing only intermediated access to CTPs;
- A review of the assessments made by CTPs of their participants for "appropriateness" from the perspective of:
  - KYC,
  - AML/CFT, and
  - product suitability; and
- Consideration of whether CTPs should provide risk disclosure, and, if so, assessing the adequacy of such disclosure.

## **2. Safeguarding Participant Assets**

*Where a CTP holds participant assets, a key consideration for regulatory authorities is how such assets are held and safeguarded. This includes consideration of what arrangements are in place in the event of a loss, including a loss due to theft from, or the bankruptcy of, the CTP.*

Many operational models for CTPs involve custody of (i.e., holding, controlling and safekeeping) participant assets, which may include crypto-assets and/or fiat currency or funds. In some cases, participant crypto-assets are held in wallets<sup>24</sup> where the CTP states that it controls the private key and thus has exclusive control over the movement of the crypto-assets. The operational models may also include other functions related to custody such as the transfer of participant funds or crypto-assets between participants and the transfer of participant funds or crypto-assets in or out of the CTP.

Asset custody functions are not usually performed by Trading Venues but rather by intermediaries, custodians, transfer agents and clearing houses. As a result, the performance of these functions directly by CTPs raises new issues and potential risks for regulatory authorities to consider.

<sup>24</sup> A crypto-asset wallet is an address, defined by its public key, which can send and receive related crypto-assets. It is secured by a private key which may only be known by the wallet owner and must be used to sign a transaction before it can be sent.



(a) *Custody of Assets and Protection against Loss*

CTPs currently use three common models of custody for crypto-assets:

- The CTP offers custody services and may hold crypto-assets in hot or cold storage;<sup>25</sup>
- Custody services are provided by a third party; or
- Participants self-custody their crypto-assets in their own wallets (and control the private keys).

The CTP model may also necessitate the holding of participant funds in the form of fiat currency.

Where the CTP offers custody, the risks that could arise include:

- *Operational failure* – the system may be compromised such that participant assets are lost or inaccessible (e.g., due to a cyber-attack).
- *Theft, loss or inaccessibility of private keys* - private keys are compromised (e.g., due to a cyber-attack or breach, or by an action of a CTP insider), lost or not accessible resulting in stolen or inaccessible assets.
- *Co-mingling of assets* – the assets of the CTP may be co-mingled with those of participants and/or participant assets may be pooled, thus in the event of a default, investor assets may not be fully protected.
- *Inaccurate record-keeping* - the CTP may not accurately reconcile records or properly account for assets.
- *Insufficient assets to meet liabilities* – the CTP may not maintain sufficient assets to cover participants' claims (i.e., the CTP is not able to meet withdrawal demands).

As noted above, Trading Venues, unlike intermediaries, do not generally have custody of participant assets. Accordingly, the Methodology for IOSCO Principle 31 relating to market intermediaries provides useful guidance for evaluating the issues and risks of CTPs offering custody of assets. In particular, Key Issue 7 of Principle 31 states:

*Where a market intermediary has control of, or is otherwise responsible for, assets belonging to a client which it is required to safeguard, it should make adequate arrangements to safeguard clients' ownership rights (for example, segregation and identification of those assets). These measures are intended to: provide protection from defalcation; facilitate the transfer of positions in cases of severe market disruption; prevent the use of client assets for proprietary trading or the financing of a market intermediary's operations; and assist in orderly winding up of the insolvency of an individual market intermediary and the return of client assets.*

CTPs' policies and procedures relating to their role in holding crypto-assets are important to consider in determining whether there are sufficient protections for participant assets. Where a CTP has exclusive control of the private keys of wallets holding participant crypto-assets, how such control can be demonstrated and audited are also important considerations.

More specifically, regulatory authorities may want to consider:

---

<sup>25</sup> Hot storage (or a hot wallet) is connected to the internet, while assets stored in cold wallets have no online connectivity.

- The types of crypto-assets the CTP has custody of;
- The lifecycle and audit trail of the movement of funds and crypto-assets between the participant, the CTP, and any third parties, and within the CTP, including in whose name the assets are stored, and whether they are stored online or offline;
- Who has access to the private keys for all CTP wallets and what backup arrangements are in place to avoid single points of access;
- Whether the funds and/or crypto-assets are segregated or pooled (and on what basis);
- What ownership rights and claims an investor has to their assets and how they are evidenced; and
- How and under what conditions assets, where crypto-assets or funds, can be withdrawn from the CTP.

In addition, there may be concerns about what procedures the CTP has in place in the event of a loss of participant assets, including a loss due to theft, bankruptcy or insolvency of the CTP. Similarly, any protections in place to compensate investors (e.g., an asset protection plan, or compensation fund or scheme) and whether the CTP has adequate financial resources to ensure an orderly wind down in the case of an insolvency are important considerations.

Further, it is important for regulatory authorities to understand the process used by a CTP to maintain accurate records and accounts of participant assets. The use of DLT may enable CTPs to provide auditable reports that verify asset holdings, but how this may occur is not always clear.

If CTPs hold participant assets, technology governance and cyber security and resilience are also important. This is discussed in more detail in section 7 below.

Lastly, an important investor protection issue and enforcement consideration relates to the geographical location of a CTP and the location where a CPT holds participant crypto-assets and/or funds and how those assets are held. It is important to consider the risks and issues relating to retrieval of participant assets and relevant disclosures to participants. The potential impact and risks in relation to the existence and/or applicability of any asset protection or insolvency regimes may also be relevant considerations.

## **Toolkit**

If a regulatory authority is considering the issues and risks associated with the safeguarding of participant assets, an assessment may include:

- A review of the adequacy of the arrangements by a CTP that:
  - discloses participant ownership rights;
  - secures participant assets in a manner that protects them from theft or loss, including appropriate backup arrangements regarding access to the private keys of CTP wallets;
  - segregates participant assets (from CTP operator assets and/or other participant assets); and
  - maintains accurate and reliable records that are sufficient to confirm participant positions;
- Where the CTP uses a third party for custody of participant assets, the adequacy of measures taken by the CTP relating to the security of the assets held at the third party;

- A review of the arrangements in place to compensate participants in the event of a loss of assets, including, for example, insurance policies, compensation funds or other contingency measures;
- An examination of the methods of retrieval of participant assets held outside of the regulatory authorities' geographical jurisdiction; and
- A consideration of the adequacy of disclosure made by the CTP to its participants in regard to the above.

*(b) Financial Resources*

*Where a CTP holds participant assets, a key consideration for regulatory authorities is whether prudential mechanisms are in place to support the operations of the CTP.*

Having sufficient financial resources fosters both confidence in markets and investor protection. Imposing capital requirements to protect against bankruptcy or insolvency is an approach that is usually reserved for intermediaries that hold investor assets. However, where a CTP holds participant assets, this may be a relevant consideration in the management of risks associated with its business model.

Where a CTP holds participant assets, IOSCO Principle 30 and the associated Key Issues that are applicable to intermediaries provide useful guidance. The Key Issues discuss initial and ongoing capital requirements for intermediaries that are directly related to the nature of the business and the risks being assumed. Where a CTP holds participant assets, capital requirements may be one mechanism to ensure that it has sufficient operational resources. In addition, where the CTP, or its operator, trades on the CTP for its own account and establishes proprietary positions in crypto-assets, there may be increased financial risk assumed by the CTP.

Maintenance of accurate and reliable records that can easily identify CTPs' capital positions at any point in time is also an important consideration.

**Toolkit**

If a regulatory authority is considering the issues and risks relating to the adequacy of the financial resources of CTPs, an assessment may include:

- Consideration of the imposition of:
  - capital requirements on CTPs that reflect the nature of the business of the CTPs, including where the CTPs perform intermediary functions;
  - ongoing monitoring of capital positions; and
  - performance of an independent audit of the CTP's financial position.

**3. Conflicts of Interest**

*A key consideration for regulatory authorities is the extent to which conflicts of interest exist due to the internal structure and organization of a CTP and, if so, how they are managed.*

The existence of unmitigated conflicts can negatively impact investor protection and confidence, as well as fair, efficient and transparent markets. The need to mitigate and manage conflicts of interest, real or perceived, is not unique to CTPs. In fact, some of the conflicts that arise with Trading Venues may also arise with CTPs. However, some conflicts may be unique.

Both Trading Venues and CTPs may have conflicts that arise from the commercial interests of the platform or venue, its owners and operators, the businesses that raise capital on the platform or venue, and the participants who trade on the platform or venue. Those CTPs that position themselves to provide end-to-end services including, for example, the admittance and trading of the crypto-asset, settlement, custody, market making and advisory services may have additional conflicts. Traditionally, these roles have been performed by independent parties. When CTPs provide such end-to-end services, any conflicts of interest that arise need to be mitigated to prevent potential market conduct and/or investor protection concerns.

In addition, issues related to market integrity and fairness may arise where a CTP's role, and therefore potential conflicts of interest between the CTP and its participants, is not transparent.

Examples of potential conflicts can include:

- *Proprietary trading and/or market making on the CTP by CTP operators, employees or affiliates* - conflicts could include information asymmetry, market abuse and/or unfair pricing provided to participants.<sup>26</sup>
- *Providing advice to customers* – this may be an inherent conflict where the CTP has a direct or indirect interest in a crypto-asset traded on the CTP, or its issuance.
- *Preferential treatment* – conflicts arise where preferential treatment is given to a subset of participants or to the owners/operators of the CTP, including system design and programming that determines how orders interact and execute.

While IOSCO Principle 31 applies to intermediaries, it is useful for the identification and management of possible conflicts of interest for CTPs. For example, Key Issue 5(d) of Principle 31 states that with regard to an intermediary's internal organization, the regulatory framework should require the following to be considered:

*Addressing any conflicts of interest that arise between [a market intermediary's] interests and those of its clients. Where the potential for conflicts arise, a market intermediary should ensure fair treatment of all its clients by taking reasonable steps to manage the conflicts through organizational measures to prevent damage to its clients' interest, such as: internal rules, including rules of confidentiality; proper disclosure; or declining to act where conflict cannot be resolved.*

A consideration of the potential conflicts of interest that may arise due to the operational structure of a CTP is important, as well as any steps taken to mitigate and manage any potential conflicts of interest between the various stakeholders, and any related disclosure.

---

<sup>26</sup> This conflict is dependent on the model of operations for a CTP. In some jurisdictions, it does not exist for Trading Venues, as proprietary trading by market operators is not permitted.

## Toolkit

If a regulatory authority is considering issues and risks relating to conflicts of interest, an assessment may include:

- An evaluation of the policies and procedures of a CTP that are established to mitigate and manage the conflicts of interest of various stakeholders, including a review of:
  - the disclosure of all relevant details, including where a CTP or related parties, or the operator, employees, officers and/or directors of the CTP or its related parties, may have any financial interest in the crypto-assets traded on that CTP; and
  - policies and procedures regarding access to and the confidentiality of information about participants on the CTP, or other information that should be treated as confidential;
- Where a CTP or related parties, or the operator, employees, officers and/or directors of the CTP or its related parties, are permitted to engage in proprietary trading and/or market making on the platform, a review of:
  - the disclosure of relevant trading activities;
  - the separation of market making activities from trading activities or services provided to participants;
  - the transparency of policies and procedures that address, among other things, participant priority, the fair pricing of trades with participants and/or favorable execution of trades with participants; and
  - disclosure relating to whether an issuer of a crypto-asset or related party is a participant on the platform; and
- A review of the disclosure of steps taken to mitigate and manage any conflicts of interest.

### 4. Description of CTP Operations

*Due to the prevalence of non-intermediated access to CTPs, a key consideration for regulatory authorities is the extent to which information about how CTPs operate is available to their participants.*

Risks due to a lack of understanding of CTP operations can arise in the absence of clear and transparent rules, policies or other documentation, including those related to price discovery,<sup>27</sup> order interactions, market making arrangements and requirements and mechanisms designed to ensure orderly trading such as trading halts. Specifically, where investors directly access the CTP and there is insufficient information available to regulators and/or investors, there may be market integrity and/or fairness issues.

As with Trading Venues, to facilitate fair and orderly trading and investor protection, transparency of a CTPs' trading operations could benefit participants. It is important for participants to have sufficient information to make informed decisions about whether to trade

---

<sup>27</sup> For example, how prices on CTPs are determined, in particular where quotes are created by the CTP operator or an affiliate acting in the capacity of a market maker.

on the CTP. This is particularly important where the CTP provides non-intermediated access to retail investors.

Key Issue 5 of IOSCO Principle 33 provides useful guidance in addressing these risks. It states:

*The order execution rules, as well as any cancellation procedures, should be disclosed to the regulator and to market participants, and should be applied fairly to all participants. The exchange or trading system's order routing procedures should also be clearly disclosed to the regulator and to market participants, applied fairly, and should not be inconsistent with relevant securities regulation (e.g., client precedence or prohibition of front running or trading ahead of customers).*<sup>28</sup>

Given that many CTPs support non-intermediated access, the extent to which information about CTP operations, including rules, policies and procedures that facilitate fair and orderly trading and investor protection is available and transparent, is an important consideration.

The use of DLT may limit the ability to cancel or modify trades once verified on the ledger. Therefore, how CTPs handle error trades<sup>29</sup> and cancellations and modifications are also important considerations. Further, the technology underlying crypto-assets may raise some novel and unique issues, such as in relation to hard forks,<sup>30</sup> airdrops<sup>31</sup> and other asset issuances, which may present operational challenges for CTPs and their participants. Specifically, hard forks make previous versions of the protocol invalid and may create entirely new assets.<sup>32</sup> Issues may arise when there is a lack of clarity about how forked crypto-assets are managed by the CTP. Where a CTP holds custody of a participant asset that can be forked, depending on the operational approach of the CTP, the participant may not have access to any new asset that results from the hard fork.

An additional risk may arise where a CTP does not have sufficient understanding of the underlying technologies used and/or the design of the crypto-assets that it makes available to trade. Specifically, if the underlying technology is immature and vulnerabilities cannot be addressed, a crypto-asset may be exposed to risks including hacking and alteration of transaction records. Additionally, if a crypto-asset is designed to be less traceable, trading activity could be used to facilitate criminal activity such as money laundering.

The availability of information describing the crypto-assets offered for trading by a CTP and any related selection criteria are also important issues to consider. This lack of information may extend to the fees charged by CTPs, which may not be clear to participants.

---

<sup>28</sup> Key Issue 5 also notes that not all jurisdictions grant SRO obligations to markets. The specific responsibilities of a market will always be defined by the applicable laws and regulations.

<sup>29</sup> See: IOSCO *Final Report on Error Trades*. Published at:  
<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD208.pdf>.

<sup>30</sup> A fork refers to a change of the code in the underlying protocol which is incompatible with the previous version. This results in different versions of the protocol.

<sup>31</sup> A crypto-asset airdrop refers to a distribution of a crypto-asset to digital wallets (often for no financial consideration).

<sup>32</sup> The October 2018 FSB report *Crypto-asset markets: Potential channels for future financial stability implications* defines a hard fork as a change to a (DLT) protocol that requires all nodes or users to upgrade to the latest version of the protocol software, or creates two versions of the protocol going forward (published at: <http://www.fsb.org/wp-content/uploads/P101018.pdf>).

## Toolkit

If a regulatory authority is considering the issues and risks relating to the transparency of CTP operations to participants, an assessment may include a review of the disclosure related to:

- Order types and interaction;
- Price discovery and transparency of orders and trades on the CTP, including trading volumes and turnover;
- Fees charged by the CTP;
- Rules relating to the prevention of market abuse;
- The technology used by the CTP;
- Policies and procedures relating to error trades, cancellations, modifications and dispute resolution;
- The treatment of assets where the distributed ledger has undergone a hard fork, or other irreversible changes to the distributed ledger protocol that makes previously valid ledgers or transactions invalid;
- The treatment of airdrops, corporate actions or other comparable events; and
- Information about the crypto-assets that the CTP offers for trading, including:
  - initial and on-going criteria for selection;
  - the principals or issuing developers behind the crypto-assets;
  - the type and details of the DLT and/or protocol used;
  - any hacking vulnerabilities of the technology underlying the crypto-assets; and
  - the traceability of the crypto-assets.

### 5. Market Integrity

*A key consideration for regulatory authorities is the applicability of existing rules relating to market abuse and the capacity of CTPs to prevent and/or detect market abuse.*

Trading Venues typically have rules governing trading and mechanisms for monitoring trading and enforcing their rules. Without these elements, there is a risk of fraud, manipulation and/or market misconduct that could be detrimental to investors and fair and efficient markets.

Key Issue 2 of IOSCO Principle 33 provides useful guidance regarding these risks. It states, in part:

*The regulator should assess the reliability of all the arrangements made by the operator for the monitoring, surveillance and supervision of the exchange or trading system and its members or participants to ensure fairness, efficiency, transparency and investor protection, as well as compliance with securities legislation.*

Also relevant is IOSCO Principle 36, which reinforces the importance of sufficient oversight. Principle 36 further notes that market manipulation, misleading or other fraudulent and deceptive conduct may result in information asymmetries, distort the price discovery process and/or prices and unfairly disadvantage investors.

Effective monitoring of trading on CTPs may be challenging. The methods for the transfer of beneficial ownership on CTPs often differ from those on Trading Venues. Therefore, rules relating to manipulation or insider trading, and how to enforce such rules, may need to be assessed as new forms of manipulation may occur. Existing supervisory tools may also need to be considered to account for unique issues relating to crypto-assets, such as the high price volatility of crypto-assets relative to traditional financial assets, the possibility of trading 24 hours a day and the lack of consistent and stable sources of crypto-asset pricing to support market surveillance systems and activities.

All of these concerns mean that the mechanisms that are used to monitor trading and whether effective monitoring is in place to detect and/or prevent fraud, manipulation or market misconduct are important considerations. Regulatory authorities may also consider how existing regulatory approaches apply to the unique characteristics of crypto-asset trading, to the extent permitted by law.

### **Toolkit**

If a regulatory authority is considering issues relating to market integrity, an assessment may include a review of:

- Traditional market integrity rules with a view to their applicability to crypto-asset trading;
- The rules, policies or procedures in place to govern trading on the market;
- Mechanisms for monitoring the rules, policies or procedures;
- The trading hours of the CTP and how they may impact the CTP’s ability to effectively monitor trading;
- The management of any information asymmetries; and
- The availability of updated information regarding factors that may impact the asset, the value of the asset, its developer or the technology used.

## **6. Price Discovery**

*A key consideration for regulatory authorities is how efficient price discovery is supported on CTPs.*

IOSCO Principle 35 provides that regulation should promote the transparency of trading. The Methodology provides that market transparency “is generally regarded as central to both fairness and efficiency of a market, and in particular to its liquidity and quality of price-formation.” However, the Methodology also notes that establishing market transparency standards is not always straightforward and that regulatory authorities need to assess the appropriate level of transparency of any particular market structure with considerable care.<sup>33</sup>

<sup>33</sup> See Transparency and Market Fragmentation, Report of the Technical Committee of IOSCO, November 2001, pp. 4–5, available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD124.pdf>. See also Transparency of Structured Finance Products, Final Report, Report of the Technical Committee of IOSCO, July 2010, p. 21, available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD326.pdf>. Principles for Dark Liquidity, *supra*, p. 26



IOSCO Principle 35 and the related Methodology discussion provide useful guidance to regulatory authorities when examining the issues relating to transparency, price discovery and the existing trading models used by CTPs. An additional challenge to the price discovery process may arise where a crypto-asset trades on multiple CTPs and/or in multiple jurisdictions. The absence of effective arbitrage mechanisms to align prices between CTPs could make the price discovery process more complex and fragmented.

However, due to the early stage of development of the crypto-asset market, it may be premature to determine the appropriate level of transparency at this point in time. Accordingly, the level of transparency is an important issue to monitor.

## **Toolkit**

If a regulatory authority is considering issues and risks relating to price discovery, an assessment may include consideration of:

- Whether and what pre- and/or post-trade information is made available to participants and/or the public and, on what basis;
- The overall potential impact of pre- and post-trade transparency on order execution quality for participants and market quality generally;
- The market microstructure of the CTP (e.g., continuous auction, call market, reference price model); and
- The crypto-assets traded, including the liquidity of the crypto-assets and their characteristics.

## **7. Technology**

Because of the nature of CTPs, the system resiliency, reliability and integrity as well as cyber resilience and security of their trading systems are critical components in managing trading risks, facilitating investor protection, and fostering fair and efficient markets. However, compared to Trading Venues, there may be unique issues and risks for CTPs, as a result of differences in technology and business models.

### *(a) Systems Resiliency, Reliability and Integrity*

*A key consideration for regulatory authorities is the mechanisms used by CTPs to facilitate resiliency, integrity and reliability of critical systems.*

System resiliency, reliability, integrity and security are important investor protection, market integrity and financial stability issues to consider in relation to both Trading Venues and CTPs.

As noted above, unlike Trading Venues, CTPs often hold participant assets and funds. Accordingly, the infrastructure and/or processes for the safeguarding of these assets and funds, are important considerations because inadequate technology and procedures could heighten the risk of loss to participants. Moreover, failure of the technology of the CTP could lead to the inaccessibility or loss of participant assets.

Accordingly, considerations such as mechanisms used by CTPs to ensure the resiliency, integrity and reliability of critical systems and business continuity/disaster recovery plans designed to ensure uninterrupted provision of services are important. IOSCO issued recommendations and sound practices relevant to Trading Venues, which are set out in the IOSCO paper entitled *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity*<sup>34</sup> and offer useful guidance in considering the issues for CTPs.

In addition, Key Issue 2 of Principle 33 provides additional guidance. It states, in part, that:

*In order to provide an appropriate level of stability, regulatory authorities should require trading venues to have in place mechanisms to help ensure the resiliency, reliability and integrity (including security) of critical systems. While the prevention of failures is important, trading venues should also be required to be prepared for dealing with such failures and, in this context, establish, maintain and implement as appropriate a Business Continuity Plan.*

Although stress testing and capacity and performance planning may not be relevant for all CTPs and crypto-assets, such processes may be important for ongoing monitoring and review. However, there may be a lack of available expertise in order to assure the operational resilience of technology and internal controls of the CTP (i.e., systems auditors).

Finally, a relevant consideration for regulatory authorities may be whether CTP systems have been developed in-house or whether any parts of the system have been acquired or licensed from a third-party. This is particularly relevant where a CTP is holding participant assets. If a CTP is using third-party services as part of its trading operations, Key Issue 3 of Principle 33 provides useful guidance in relation to outsourcing by Trading Venues, and states:

*When functions are outsourced, such outsourcing does not negate the liability of the outsourcing market for any and all functions that the market may outsource to a service provider. The outsourcing market must retain the competence and ability to be able to ensure that it complies with all regulatory requirements. Accordingly, with respect to the outsourcing of key regulatory functions, markets should consider how and whether such functions may be outsourced. Outsourcing should not be permitted if it impairs the market authority's ability to exercise its statutory responsibilities, such as proper supervision and audit of the market.*

## **Toolkit**

If a regulatory authority is considering issues and risks relating to system resiliency, integrity and reliability, an assessment may include a review of:

- The CTP's business continuity/disaster recovery plans to ensure continuity of services;
- Where appropriate, stress testing and/or capacity planning processes and results;
- Quality assurance procedures and performance monitoring of any critical systems that are provided or developed by third-parties (whether or not outsourcing agreements are in place);
- Governance and change management procedures; and

---

<sup>34</sup>

Published at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf>

- Independent systems reviews to assure that relevant technology standards are met and maintained as intended.

(b) *Cyber Security and Resilience*

*A key consideration for regulatory authorities is how a CTP addresses cyber security and resilience.*

A key issue for all market participants is cyber security and resilience. Cyber incidents have become more frequent and complex in nature. Thus, measures to protect against cyber incidents are important for both Trading Venues and CTPs but may be particularly important for CTPs due to the use of novel technology and the fact that many CTPs hold participant assets. Security breaches and the exploitation of system vulnerabilities of CTPs and wallets have resulted in significant losses of investor assets.<sup>35</sup> These risks may increase if the CTP stores participant assets in a hot wallet. In addition, where investors, including retail investors, are on-boarded and provide personal information, cyber vulnerabilities may be exploited to access that individual information.

The existing regulatory requirements relating to cyber security and resilience may apply to CTPs in some jurisdictions. The CPMI-IOSCO report *Guidance on Cyber Resilience for Financial Market Infrastructures*,<sup>36</sup> the National Institute of Standards and Technology (NIST) Framework for improving Critical Infrastructure Cybersecurity,<sup>37</sup> the International Organization for Standardization (ISO) 27000 series standards and the G-7 published *Fundamental Elements of Cybersecurity for the Financial Sector*<sup>38</sup> may provide useful guidance for enhancing CTP cyber security and resilience.

To manage the risks, consideration of whether CTPs have implemented appropriate policies, procedures and security controls for trading and, if applicable, custody systems, and whether such systems and controls are regularly assessed for effectiveness is important. In addition, regulatory authorities might consider whether CTPs have an overall level of understanding within the organization to identify critical systems and assets and have established the appropriate risk management controls, and support ongoing education regarding evolving cyber threats.

### **Toolkit**

If a regulatory authority is considering the issues and risks associated with cyber security and resilience, an assessment may include consideration of a CTP's:

<sup>35</sup> See, e.g., Tan, Andrea and Yuji Nakamura. "Cryptocurrency Markets Are Juicy Targets for Hackers: Timeline" *Bloomberg*, Bloomberg L.P., 20 June 2018, <https://www.bloomberg.com/news/articles/2018-06-20/cryptocurrency-markets-are-juicy-targets-for-hackers-timeline>

<sup>36</sup> <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>

<sup>37</sup> <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

<sup>38</sup> <https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf>.

- Policies and procedures that support an appropriate governance structure that identifies key systems or assets that could be at risk;
- Physical or organizational measures to control and protect against cyber risks (e.g., vulnerability testing, penetration testing);
- Measures to detect cyber anomalies;
- Policies related to incident response; and
- Business continuity plans and/or disaster recovery plans.

## 8. Clearing and Settlement

Efficient and reliable clearing and settlement of transactions is critical to investor protection, fair and efficient markets and financial stability. While certain DLT systems could potentially increase the efficiency of existing clearing systems, these processes present potentially novel considerations for regulatory authorities in relation to crypto-asset trading, and are important considerations.

With respect to clearing, some CTPs may maintain and update the account balances of participants on that CTP. While a separate party, like an intermediary, may assume this role for traditional securities, some CTPs may integrate these services into its operations. In such cases, efficient and accurate internal accounting systems are important for CTPs, especially where they provide non-intermediated access and allow for automated participant withdrawals. If accounting systems are inaccurate or compromised, withdrawals might be made by without ownership of the assets.

Similarly, it is important to understand how transactions that occur on CTPs are settled. Due to the underlying technology and trading models of CTPs, it may be unclear whether traditional settlement mechanisms are necessary or utilized to effect transfers of crypto-asset ownership. For example, how settlement finality is reached when recording transactions in a distributed ledger is important and may vary. In addition, it is currently unclear whether there is a common understanding or agreement of when legal transfer of ownership occurs when crypto-assets are trading on CTPs.

CTPs policies and procedures that address ownership and liability across the lifecycle of the movement of funds and assets between the participant, the CTP, and any third parties, and within the CTP are important. In addition, policies and procedures that address potential issues such as delays, complications or costs are important considerations. For example, in the case of a “51% attack”<sup>39</sup> or similarly targeted disruption, it is important for the CTP to confirm who is responsible for issues that may arise during the transfer process.

Depending on the CTP’s arrangements for clearing and settlement, IOSCO Principle 38 provides useful guidance. Where there are clearing and settlement processes in place for trading crypto-assets on CTPs, it is important to understand the processes involved. In April 2018, the Committee on Payments and Market Infrastructures and IOSCO (CPMI-IOSCO) Joint Working Group on Digital Innovations (JWGDI) examined whether initiatives using DLT in clearing and settlement pose challenges for the application of the Principles for Financial

---

<sup>39</sup> A 51% attack can occur when a singular actor or alliance of actors gains enough control of a DLT’s consensus mechanism to create a differing version of the DLT that must be accepted by other participants. Actors may choose to perform a 51% attack to double spend assets or to create new assets for themselves against protocol specifications. Attackers may also wish to corrupt the chain for nefarious purposes.

Market Infrastructures (PFMI)<sup>40</sup>. The report did not identify any issues or gaps in the PFMI regarding the current use of DLT by financial market infrastructures. In this area, Committee 2 will defer to the on-going monitoring of the CPMI-IOSCO.

---

<sup>40</sup> Published at: <https://www.bis.org/cpmi/publ/d101a.pdf>

## 5. Cross-border Information Sharing

As previously noted, similar to the trading of traditional financial instruments, the trading of crypto-assets may span geographic borders. Crypto-asset trading takes place 24 hours a day with investors, participants, intermediaries and platforms from around the world. IOSCO members have agreed to:

- Cooperate in developing, implementing and promoting adherence to internationally recognized and consistent standards of regulation, oversight and enforcement in order to protect investors, maintain fair, efficient and transparent markets, and seek to address systemic risks;
- Enhance investor protection and promote investor confidence in the integrity of securities markets, through strengthened information exchange and cooperation in enforcement against misconduct and in supervision of markets and market intermediaries; and
- Exchange information at both global and regional levels on their respective experiences in order to assist the development of markets, strengthen market infrastructure and implement appropriate regulation.

Some of the issues relating to the regulation of Trading Venues also arise with respect to CTPs. Specifically, there is the risk of regulatory arbitrage, the risk that an unregulated CTP operates and provides access to participants and the risk that a CTP provides access to participants in a jurisdiction in which this is not permitted. These risks highlight the need for appropriate cooperation and communication between regulatory authorities seeking to ensure investors are protected.

While regulatory authorities may have different supervisory approaches, effective information sharing and cooperation is important to manage the risks associated with this global trading of crypto-assets. Where the operations of CTPs involve multiple jurisdictions, and information sharing arrangements exist, regulatory authorities could share information and communicate information about CTP operations, to the extent permitted by such information sharing arrangements and any applicable legal requirements. They could also share information and cooperate with respect to enforcement investigations and proceedings undertaken, and to coordinate to the extent permitted by existing arrangements.

For many jurisdictions, the arrangements for cooperation and sharing are in place already.<sup>41</sup>

- In connection with information sharing relating to enforcement investigations, the *Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information* (IOSCO MMoU) and the *Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information* (EMMoU) facilitate the exchange of information. They are the key instruments used by securities regulatory authorities that

---

<sup>41</sup> In addition to formal cooperation and sharing arrangements, IOSCO has established an information repository of supervisory cooperation MoUs entered into by its members and these will cover trading in crypto-assets to the extent that they are within their scope. This repository is aimed at assisting IOSCO Members in developing bilateral arrangements, which may foster multilateral or new approaches in areas such as crypto-asset trading. Further, the FSB has also published a crypto-assets regulators directory which aims to provide information on the regulators and authorities in FSB jurisdictions and standard-setting bodies who are dealing with crypto-asset issues.

are signatories to the MMoU or EMMoU globally to request assistance in securing compliance with, and enforcing securities and derivatives laws.<sup>42</sup>

- Many regulatory authorities have bilateral Memoranda of Understanding with other regulatory authorities that facilitate information sharing. However, the exchange of information under bilateral Memoranda of Understanding depends on whether the relevant CTP falls within the regulatory jurisdiction of both the signatories and is covered by such arrangements.
- The IOSCO Board and Committees share information on a regular basis relating to trading in secondary markets, enforcement, and intermediaries, including in relation to crypto-assets.
- As noted above, the IOSCO Board established the ICO Network which shares experiences with respect to the regulation of crypto-assets with a focus on initial coin offerings.

IOSCO Principles 13, 14 and 15 apply to the trading of financial assets, including crypto-assets that are securities. They specifically address cooperation of securities regulatory authorities, whether domestic or foreign, with respect to information relating to investigations and enforcement. In the specific context of CTPs, secondary market trading and manipulation or other unfair trading practices, Key Issue 4 of IOSCO Principle 36 provides useful guidance. It states:

*There must be adequate information sharing between relevant regulatory authorities, sufficient to ensure effective enforcement.*

In addition, the general principles in IOSCO's report entitled *Principles Regarding Cross-Border Supervisory Cooperation*<sup>43</sup> may apply to CTP oversight where the CTP operates across borders. These principles can assist when regulatory authorities develop cooperation arrangements.

---

<sup>42</sup> See: *IOSCO Task Force on Cross-Border Regulation Final Report*, published at: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD507.pdf>

<sup>43</sup> <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD322.pdf>

## Chapter 6 - Conclusion

As discussed in this Consultation Report, many regulatory authorities globally are considering issues relating to the trading of crypto-assets on CTPs. Where a regulatory authority has determined that a crypto-asset is a security and falls within its remit, the basic principles or objectives of securities regulation should apply. The IOSCO Principles and Methodology provide useful guidance in considering the issues, risks and key considerations identified in this report.

The crypto-asset market is evolving and the Consultation Report outlines risks and issues that have been identified thus far and sets out key considerations that may be relevant for regulatory authorities that are considering the potentially novel and unique issues related to the regulation of CTPs. The Consultation Report also provides a corresponding toolkit of possible measures that may be considered or used to address the underlying risks.

These key considerations relate to:

- Access and on-boarding;
- Safekeeping of participant assets, including custody arrangements;
- Identification and management of conflicts of interest;
- Transparency of operations;
- Market integrity, including the rules governing trading on the CTP, and how those rules are monitored and enforced;
- Price discovery mechanisms;
- Technology, including resiliency and cyber security.

As noted above, these key considerations are dependent on the operational model of the CTP and may already be mitigated or addressed by existing regulatory frameworks. Many Committee 2 member jurisdictions indicated that where a crypto-asset would fall under their regulatory remit, existing regulatory frameworks would apply (including requirements applicable to Trading Venues). However, some jurisdictions are considering new or tailored requirements to account for the novel and unique characteristics of CTPs.

IOSCO intends to continue to monitor the evolving crypto-asset market, with a view to ensuring the risks and issues and the key considerations identified continue to be appropriate and relevant.



## **Annex A**

Many IOSCO members have provided information about what they have published with respect to their regulatory framework applicable to CTPs that are within their jurisdiction.

### **Abu Dhabi**

On May 14, 2019, Abu Dhabi published an updated guidance note on the Regulation of Crypto-Asset Activities in Abu Dhabi Global Market (ADGM).

[https://www.adgm.com/media/327606/guidance-regulation-of-crypto-asset-activities-in-adgm\\_v20\\_20190514.pdf](https://www.adgm.com/media/327606/guidance-regulation-of-crypto-asset-activities-in-adgm_v20_20190514.pdf)

### **Australia**

In May 2018, ASIC released Information Sheet 225 (INFO 225) giving guidance about the potential application of the Corporations Act 2001 (Corporations Act) to entities that are considering raising funds through an initial coin offering (ICO) and to other crypto-currency or digital token (referred to as 'crypto-asset') businesses. Part C covers when a crypto-asset trading platform could be a financial market.

<https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-currency/#trading>

### **Canada**

On March 14, 2019, the Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada published a consultation paper on a proposed framework for Crypto-Asset Trading Platforms, seeking input on how regulatory requirements may be tailored for CTPs operating in Canada.

[https://www.osc.gov.on.ca/en/SecuritiesLaw\\_csa\\_20190314\\_21-402\\_crypto-asset-trading-platforms.htm](https://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20190314_21-402_crypto-asset-trading-platforms.htm)

### **China**

In September 2017, the Announcement on Guarding against ICO Risks, jointly issued by 7 ministries including the People's Bank of China, clearly pointed out that ICO activities are suspected of involving illegal criminal activities including illegal fund-raising, illegal issuance of securities, and illegal sale of notes and bonds, and that all institutions and individuals should immediately stop engaging in ICO activities.

<http://www.pbc.gov.cn/en/3688110/3688181/3712144/index.html>

### **France**

The AMF follows a dual approach depending on the nature of the asset. If the crypto-asset is defined as a financial instrument, the platform will fall under existing financial market regulations. Otherwise, for non-security crypto-assets, notably regarding tokens that do not fall under any existing regulations, the AMF supports the development of a bespoke regime. Hence, the French Finance Minister has presented to the French Parliament a draft law called 'PACTE' setting out a legal framework for initial coin offerings and for crypto services providers.

At this stage, the AMF considers that the vast majority of currently traded crypto-assets do not fall within the scope of the legal definition of a ‘security’.

These first views were expressed in the summary of replies to the public consultation on ICOs issued on 22 February 2018.

[https://www.amf-france.org/en\\_US/Actualites/Communiqués-de-presse/AMF/annee-2018/retour-de-consultation-ICO/EN](https://www.amf-france.org/en_US/Actualites/Communiqués-de-presse/AMF/annee-2018/retour-de-consultation-ICO/EN)

In the meantime, the AMF has published several warnings to investors regarding risks related to crypto-assets, mentioning risks related to CTPs.

<https://www.amf-france.org/Epargne-Info-Service/Protéger-son-épargne/Crypto-actifs-Bitcoin-etc/Crypto-monnaies-attention-aux-arnaques>

### **Germany**

In March 2018, BaFin issued an advisory letter with respect to the classification of tokens as financial instruments as a vehicle of Initial Coin Offerings.

[https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl\\_hinweisschreiben\\_einordnung\\_ICOs\\_en.html](https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.html)

[https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa\\_bj\\_1803\\_ICOs.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1803_ICOs.html)

Further, in August 2018, BaFin issued an article on the Blockchain Technology with respect to the legal environment.

[https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp\\_18-1\\_Beitag\\_Fusswinkel\\_en.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2018/bp_18-1_Beitag_Fusswinkel_en.html)

### **Gibraltar**

Since January 1, 2018, any firm carrying out by way of business, in or from Gibraltar, the use of DLT for storing or transmitting value belong to others (DLT activities), needs to be authorized by the Gibraltar Financial Services Commission as a DLT provider.

Information about the DLT framework in Gibraltar can be found at:

<http://www.gfsc.gi/dlt>

In addition, on March 9, 2018, the Government of Gibraltar published a policy paper on token regulation, including related secondary market activities.

<http://gibraltarfinance.gi/20180309-token-regulation---policy-document-v2.1-final.pdf>

### **Hong Kong**

On November 1, 2018, the Securities and Futures Commission issued a statement setting out a new approach which aims to bring virtual asset portfolio managers and distributors of virtual asset funds under its regulatory net. It also sets out a conceptual framework for the potential regulation of virtual asset trading platforms.

<https://www.sfc.hk/web/EN/news-and-announcements/policy-statements-and-announcements/reg-framework-virtual-asset-portfolios-managers-fund-distributors-trading-platform-operators.html>

## **Israel**

On March 5, 2019, the Israel Securities Authority published the final report of the Committee to Examine the Regulation of the Issuance of Decentralized Cryptographic Currency to the Public

<http://www.isa.gov.il/sites/ISAEng/1489/1513/Documents/FinalCryptoReportENG.pdf>

## **Italy**

On March 19, 2019, CONSOB issued a document for discussion that summarizes the main items to be considered in developing a possible regulatory approach to crypto-assets.

[http://www.consob.it/documents/46180/46181/doc\\_disc\\_20190319\\_en.pdf/e981f8a9-e370-4456-8f67-111e460610f0](http://www.consob.it/documents/46180/46181/doc_disc_20190319_en.pdf/e981f8a9-e370-4456-8f67-111e460610f0)

## **Japan**

In April 2017, the Act on Prevention of Transfer of Criminal Proceeds was amended as countermeasures against money laundering and terrorist financing which obligates CTPs to identify customers. At the same time, the Japan Financial Services Agency (JFSA) established rules for customer protection by the amendment of Payment Services Act (PSA) including accountabilities of the CTPs to the customers.

<http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02>

In March 2018, the Study Group of Virtual Currency Exchange Services consisting of external experts was established to deliberate on regulatory measures for various emerging issues surrounding the CTPs, including the biggest hacking incident happened to a CTP in Japan. In December 2018, the Study Group published a report which suggests, for instance, the introduction of regulation on crypto-asset custodial services, crypto-asset CFDs and unfair acts in crypto asset spot trading, and the clarification and development of ICO related regulation.

<https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181228.html>

JFSA submitted a bill to the Diet to amend its regulatory framework applicable to CTPs in March 2019 based on the findings in the report.

<https://www.fsa.go.jp/common/diet/198/02/houritsuanriyuu.pdf> (in Japanese)

Also, in October 2018, the Japan Virtual Currency Exchange Association was certified as the certified association for payment service providers (a self-regulatory organization under the PSA) and it set up self-regulation rules.

<https://jvcea.or.jp/about/rule/> (in Japanese)

## **Malaysia**

In January 2019, SC Malaysia published a *Framework to Facilitate Trading of Digital Assets*

<https://www.sc.com.my/news/media-releases-and-announcements/sc-introduces-framework-to-facilitate-trading-of-digital-assets-in-malaysia>

Further, SC Malaysia published *Guidelines on Recognized Markets* which introduces the new requirements for electronic platforms that facilitate the trading of digital assets.

<https://www.sc.com.my/api/documentms/download.ashx?id=eb8f1b04-d744-4f9a-a6b6-ff8f6fee8701>

## **Netherlands**

On January 18, 2019, the AFM and DNB recommended regulation of crypto-assets at an international level.

<https://www.afm.nl/en/professionals/nieuws/2019/jan/adviesrapport-crypto>

## **New Zealand**

The following information has been published by the Financial Markets Authority of New Zealand.

<http://www.fma.govt.nz/compliance/cryptocurrencies/cryptocurrency-services/>

## **Singapore**

On August 1, 2017, MAS clarified (link below) that if a digital token constitutes a product regulated under the securities laws administered by MAS, the offer or issue of digital tokens must comply with the applicable securities laws. MAS subsequently issued A Guide to Digital Token Offerings (link below) on 14 November 2017 to provide guidance on how the securities laws administered by MAS would apply to the offers or issues of digital tokens in Singapore. Further, the Singapore Parliament has passed the Payment Services Act (PSA) on 14 January 2019. Under the PSA, a person carrying on a business of providing any service of dealing in digital payment tokens or any service of facilitating the exchange of digital payment tokens must be licensed and will be regulated under the PSA for AML/CFT purposes.

[http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx?utm\\_source=rss&utm\\_medium=rss](http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx?utm_source=rss&utm_medium=rss)

<http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20last%20updated%20on%2030%20Nov%202018.pdf>

## **Spain**

CNMV has published a document setting out the initial criteria that it is applying in relation to ICOs.

<http://cnmv.es/DocPortal/Fintech/CriteriosICOsEN.pdf>

On January 9, 2019, ESMA provided advice to the EU Commission on ICOs and crypto-assets.

[https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf)

## **Switzerland**

FINMA published its Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICO) on 16 February 2018

<https://www.finma.ch/en/~media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en>

## **Thailand**

The Securities and Exchange Commission, Thailand, has published the following documents in relation to digital assets:

- Emergency Decree on Digital Asset Businesses B.E. 2561: <https://www.sec.or.th/EN/Documents/ActandRoyalEnactment/RoyalEnactment/enactment-digitalasset2018.pdf>
- Regulations of Digital Asset Businesses: <https://www.sec.or.th/EN/Pages/LawandRegulations/DigitalAssetBusiness.aspx>
- List of Licensed Digital Asset Businesses: <https://www.sec.or.th/EN/Pages/Shortcut/DigitalAsset.aspx#ebd>
- Investor Alert: <https://www.sec.or.th/EN/Pages/Shortcut/DigitalAsset.aspx#Alert>
- Investor Education Website on Digital Assets: <https://i๓๓๓๓๓.com/>

### **United Kingdom**

Joint HMT/BoE/FCA TF report (Oct 2018)

The UK Government announced the Taskforce in March 2018 as part of its wider Fintech strategy and in response to the Treasury Select Committee's investigation into digital currencies. The objective of the Taskforce was to bring Her Majesty's Treasury (HMT), Bank of England (BoE) and the Financial Conduct Authority (FCA) together to assess the potential impact of crypto-assets and DLT in the UK and to consider appropriate policy responses.

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/752070/cryptoassets\\_taskforce\\_final\\_report\\_final\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf)

<https://www.fca.org.uk/news/news-stories/cryptoasset-taskforce-publishes-report-uk-approach-cryptoassets>

CP19/3 CA perimeter guidance consultation (Jan 2019)

The Taskforce set out a number of commitments, including providing extra clarity to firms about where current crypto-asset activities are regulated, and exploring whether unregulated activities should be captured by regulation in the future. This Guidance consultation document responds to the first of those commitments.

<https://www.fca.org.uk/publication/consultation/cp19-03.pdf>

### **United States - Commodity Futures Trading Commission (CFTC)**

CFTC Staff Advisory No. 18-14: Advisory with respect to Virtual Currency Derivative Product Listings:

<https://www.cftc.gov/sites/default/files/csl/pdfs/18/18-14.pdf>

### **United States – Securities and Exchange Commission (SEC)**

Statement on Digital Asset Securities Issuance and Trading (November 16, 2018)

<https://www.sec.gov/news/public-statement/digital-asset-securities-issuance-and-trading>

Statement on Potentially Unlawful Online Platforms for Trading Digital Assets (March 8, 2018)

<https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>

FINHUB: Strategic Hub for Innovation and Financial Technology

<https://www.sec.gov/finhub>

## **Annex B**

### **Summary of Key Survey Findings**

Seeking feedback in several specific areas, the Survey was sent to all member jurisdictions of Committee 2 and members of the ICO Network in late 2018. Information was requested in relation to the types of operational models of CTPs seen by each responding jurisdiction, how they were accessed (e.g., through a registered intermediary or directly by investors), if, and how assets were cleared and settled, and whether assets were custodied by the CTP. The Survey also identified specific areas of consideration and requested information about the risks associated with each area, and the related requirements or policy measures imposed or being considered (where different than current approaches for Trading Venues). Lastly, the Survey provided an opportunity for responding jurisdictions to identify any other risks or concerns relevant to CTPs.

#### **1. CTP Operational Models**

##### *(a) Structure*

Respondents noted a variety of models in relation to the operational structure of CTPs. Many are structured like the common “continuous auction” equity Trading Venues (e.g., they have central limit order books and a variety of order types that are common to equity trading). Other models included decentralized peer-to-peer trading, unilateral trading between the operator and investors and models that are more akin to order routing services. The central limit order book model was most common among respondents.

##### *(b) Access*

While responses indicated operational models offering both intermediated and non-intermediated access to CTPs, non-intermediated access to CTPs was predominant. Access is usually provided directly to investors, including retail investors.

##### *(c) Custody*

The Survey responses identified three models of crypto-asset custody:

- The CTP offers custody of the participant assets in digital wallets (“hot” and/or “cold” wallets);
- Custody services are offered by affiliated or authorized third-party service providers; and
- Self-custody, where the investor is responsible for the storage of the crypto-asset in their own wallet.

Responses indicated that the most common model is where the CTP offers custody of participant assets.

#### *(d) Clearing and Settlement*

Most responding jurisdictions did not specifically identify the existence of clearing and settlement infrastructure or processes, and noted that crypto-asset transactions are often pre-funded with no leverage or margin available.

## **2. Regulatory Approaches**

The Survey requested information regarding what regulatory approaches were in place or being considered in relation to CTPs. Responses received were largely dependent on whether the assets being traded on a CTP fell within the remit of a regulatory authority (i.e., where the asset was considered a “security”, a “financial instrument” or “asset” or a “derivative”). Many respondents indicated that they are still in the process of making this determination.

#### *(a) Application of Existing Regulatory Framework*

Where a crypto-asset qualifies as a financial instrument, most responses indicated that the existing regulatory approach would apply. A small number of respondents noted that only certain existing requirements are applicable to CTPs, in particular the application of requirements related to AML/CFT. However, some jurisdictions indicated that the existing regulatory framework does not apply to CTPs (in some cases analysis is currently being undertaken), either because the related activities do not fall within their remit or because the operation of a CTP is not permitted.

#### *(b) Tailoring of Existing Regulatory Framework*

While specific details were not typically provided, some jurisdictions noted that they are considering tailoring existing requirements to account for some unique characteristics of CTPs.

#### *(c) Introduction of a New Regulatory Framework*

A minority of respondents indicated that they have introduced or have proposed a specific framework applicable to crypto-assets and CTPs (where they are otherwise not captured under existing legislation). Only a small number of jurisdictions have already adopted new requirements to regulate CTPs while the remainder are either considering or have proposed a relevant framework. Survey responses provided were general in nature, but where new requirements have been adopted, proposed, or are being considered, responses indicate that existing regulatory regimes applicable to Trading Venues are often the basis, with additional consideration being given to unique risks or features of crypto-assets and CTPs.

## **3. Considerations and Risks**

The Survey requested information from responding jurisdictions regarding any unique risks applicable to CTPs, relative to Trading Venues.

While a number of jurisdictions responded that many risks associated with CTPs are similar to those applicable to Trading Venues, some risks were identified that were either unique, or enhanced due to nuances with crypto-assets, CTPs and/or the use of DLT. This section summarizes the Survey responses related to the risks identified.



### *(a) On-Boarding and KYC Process*

As previously noted, most jurisdictions observed that CTPs offer direct access to investors, including retail investors. This is unlike Trading Venues where the access is intermediated by an entity that is authorised by a competent authority. Survey responses indicated that standards used by CTPs to on-board clients are limited, with minimal KYC/AML checks as compared to the requirements typically imposed on intermediaries that include due diligence and verifications, among others. Responses noted that the lack of on-boarding standards may increase the risk of the CTP being used for fraudulent, criminal and illegal activities, especially where the underlying technology or DLT provides for the anonymous or pseudonymous transfer of crypto-assets between parties and/or masks the origin or destination of the crypto-assets. Another concern raised was that investors may access the platform from prohibited jurisdictions, thus presenting opportunities for jurisdictional arbitrage.

In addition, CTPs may not undertake any suitability assessments before allowing participants to trade. Some jurisdictions noted that suitability assessments including considerations such as an investor's financial situation and risk tolerance are important investor protection tools.

Although some respondents noted that AML and counter-terrorist financing regulations would apply to CTPs, associated risks were most commonly identified as unique. This was primarily due to the anonymity or pseudo-anonymity offered by DLT and/or decentralized systems, and potentially absent or deficient policies and procedures in place by CTPs when onboarding participants.

Although many noted that similar risks exist for Trading Venues, technology governance was identified by respondents as unique, in the sense that it may be enhanced due to the risk of theft or loss of investor assets where they are custodied by a CTP.

To address the above risks, most jurisdictions expressed the view that an enhanced level of regulatory focus might be necessary for CTPs that allow direct access for retail investors. Many believed that imposing certain requirements typically applicable to intermediaries could be required for CTPs, including, for example, those related to KYC, due diligence, and AML. Some questioned whether CTPs should only be accessible to institutional or high net worth investors.

Some jurisdictions have requirements related to fairness of access (e.g., transparent, non-discriminatory access criteria) that are currently applicable to Trading Venues and some noted that these requirements would apply to CTPs. Other considerations were identified in relation to the provision of risk disclosures by CTPs to retail investor participants.

### *(b) Identification and Management of Conflicts of Interest*

In general, jurisdictions noted that conflicts of interest that might be applicable to Trading Venues might also apply to CTPs. The key risk identified is that CTPs may not be able to identify, mitigate or manage potential conflicts, which could include:

- Conflicts between the commercial interests of the CTP, its owners and operators, the businesses that raise capital on the platform, and the participants who trade on the platform; and

- Conflicts arising from the platform performing proprietary trading and conflicts arising from the CTPs' owners and employees trading on the platform against CTP participants.

Depending on the business model of a CTP, more pronounced or additional conflicts may exist.

To mitigate risks, some jurisdictions cited that where crypto-assets qualify as financial instruments, existing rules applicable to Trading Venues would also be applicable to CTPs. In general, many jurisdictions expressed the view that there should be greater transparency of potential conflicts, and that CTPs should establish and maintain policies and procedures to mitigate and manage any potential conflicts of interest between the various stakeholders (as may be the case with Trading Venues). A few jurisdictions noted specific considerations including, for example, ethical walls separating proprietary trading from trading on behalf of participants, ensuring the priority of participant's orders over proprietary orders and the establishment of dispute resolution mechanisms to manage complaints from participants.

*(c) Understanding the Operations of the Platform*

As with other responses to Survey questions, some jurisdictions noted that any risks relating to a lack of understanding of the operations of a CTP are like those applicable to Trading Venues. However, some responses identified risks applicable to CTPs. Specifically, concerns were raised where investors directly access the CTP and where there is insufficient information available to investors (and regulatory authorities) regarding, for example, how orders interact, mechanisms designed to ensure orderly trading, rules regarding trading halts and/or general transparency of orders and trades on a CTP. Where there is insufficient transparency into CTP operations, market integrity or fairness risks may result.

Additional areas of risk identified include in relation to the flow of funds in and out of a CTP, trading and other applicable fees and the potential impacts of 24-hour trading on price discovery.

Some respondents indicated that no new requirements had been established for CTPs, others noted that existing regulatory frameworks would apply, and some described requirements or policy measures that have been imposed or are being considered. Some jurisdictions suggested that CTPs should publish certain information on websites including, for example, information related to:

- Trading and operational matters;
- Order types;
- Order execution methodologies;
- Rules preventing market manipulation and abusive activities;
- Volatility control mechanisms
- Policies and procedures when trading is suspended and/or an outage occurs;
- Deposit and withdrawal procedures;
- Custodial arrangements; and
- Dispute resolution mechanisms

*(d) Transparency of the Role of the CTP Operator*

Several jurisdictions noted that there may be insufficient information disclosed to participants in relation to the role of CTP operators on the platform. Based on responses received, potential risks in this regard are like those identified in relation to conflicts of interest and may give rise to market integrity or fairness issues. For example, some jurisdictions noted that where an operator of a CTP and/or its affiliates participate on that CTP, the operator and/or its affiliates are privy to market sensitive information that could be used for manipulative purposes.

Given the varied business models of CTPs, (e.g., some only operate a matching engine, others may have multiple roles such as acting as an intermediary, custody, etc.), some respondents expressed the view that an operator should provide appropriate transparency in relation to its role on its CTP.

Some respondents also took the position that CTPs have a role to play in providing greater transparency or disclosure with respect to the risks of crypto-assets and crypto-asset trading more generally, including:

- Crypto-asset price volatility;
- Risks related to the underlying technology (e.g., how trading of assets based on distributed ledger technology differs from traditional asset trading, including the possibility of irreversible transactions);
- Cyber-related risks; and
- Fraud and other technology risks.

#### *(e) Market Integrity*

The main risk identified by respondents in relation to market integrity was the potential for market manipulation and investor losses. Concerns were raised by some jurisdictions relating to a lack of disclosure regarding whether and how CTPs govern or enforce any trading standards, or to ensure that trading is fair and orderly. A related concern expressed in some responses was whether CTPs were adequately equipped to monitor trading, in terms of surveillance tools or other resources such as necessary expertise.

As with responses to other Survey questions, a number of jurisdictions indicated that where a crypto-asset qualifies as a “financial instrument”, existing regulatory frameworks would apply. Some responding jurisdictions indicated that they have implemented market integrity rules for CTPs, and many others noted that specific considerations were being undertaken to prevent market abuse, manipulation and/or fraud.

#### *(f) Price Discovery*

In relation to price discovery on CTPs, the primary risk identified by responding jurisdictions was insufficient pre- and post-trade transparency. A number of respondents noted the link between poor transparency and other risks such as best execution and efficient trading. Some jurisdictions also noted poor liquidity and/or fragmentation of trading, and referenced concerns related to a high degree of asset price variation among CTPs.

To mitigate potential risks to price discovery, some respondents reported that they were either considering, or had imposed pre- and/or post-trade transparency requirements, either through the application of existing requirements, or through the development of new requirements.

*(g) Safeguarding Participant Assets (Custody)*

Some responding jurisdictions identified risks related to custody of assets as of primary importance, expressing the view that many of the operational failures commonly attributed to CTPs should be attributed to a failure of custody arrangements, including insufficient technology governance arrangements.

Where crypto-assets are custodied by a CTP, investors may be exposed to increased risks, most notably theft or loss of assets, either through cyber-attack or through loss of private keys that could render crypto-assets inaccessible. It was noted however, that similar risks may also exist even where an investor stores crypto-assets in their own wallet, and that not all investors have the necessary expertise to undertake self-custody.

Further, some jurisdictions highlighted asset segregation as a risk, in that comingling of participant assets might result in inadequate protections in the event of a default. Other concerns included a lack of disclosure of custody procedures for CTPs, slow development of robust custody standards and a lack of investor protection funds for this asset class. Lastly, some jurisdictions highlighted a lack of clarity regarding legal ownership of crypto-assets, particularly in relation to assets held by a CTP.

In relation to risk mitigation, while a few respondents already had specific requirements in place, many jurisdictions noted that where not already subject to existing rules, they are currently considering the best approach to addressing issues related to custody. Requirements in place or being considered include:

- Establishing controls designed to safeguard participant assets and independent assurances of the effectiveness of the controls;
- Obligations to segregate assets in accounts of investors;
- Mandating frequent verification of account balances;
- Mandating use of cold storage or independent licensed custodians;
- Disclosure of how participant assets are held; and
- Determination of conditions under which legal ownership is proven.

*(h) Safeguarding Participant Assets (Financial Resources)*

Most respondents indicated that the main financial risks for CTPs relate to the business/operational continuity in the event of financial difficulties. Particularly, the following risks were highlighted by responding jurisdictions:

- Insufficient capital to support operations in case of financial difficulties (which may be particularly acute where the CTP is a small organization);
- Liquidity and solvency risk due to unexpected price fluctuation of crypto-assets traded on/held by the CTP; and
- Financial inability to cover losses due to technological failures, cyber-attacks or other unexpected events (especially in cases where the platform custodies participants' assets).

Many respondents indicated that they have already implemented, or will implement capital requirements for CTPs to guarantee the continuity of operations. For example:

- Requirements to maintain reserves to cover the cost of operations for several months as financial buffer; and
- Requirements for minimum paid-up capital and shareholders' funds.

Where they custody participant assets, some respondents noted that CTPs are exposed to higher risks related to asset loss from hacking and theft as compared to Trading Venues (that do not typically undertake custody functions). These jurisdictions highlighted the importance of CTPs having measures to compensate participants in the event of a loss. Some jurisdictions have already implemented a requirement for insurance policies, while others are considering requiring CTPs to have either insurance or their own fund sufficient to cover losses.

A few jurisdictions noted that the level of risk would significantly differ depending on how the platforms manage the private keys of wallets that hold participant assets (e.g., in hot or cold storage). Certain respondents require CTPs to provide full coverage for crypto-assets held in hot storage and substantial coverage for those held in cold storage.

*(i) System Resiliency, Integrity and Security*

Many jurisdictions noted that risks associated with system resiliency, integrity and security for CTPs are not dissimilar to equivalent risks associated with Trading Venues, but some respondent noted concerns that CTP operators may not have the same level of expertise and resources to manage the risks as compared to operators of Trading Venues. The primary risks identified include trading halts/disruptions or systems failures that could potentially result in a loss of participant assets and/or lack of investor confidence in the market.

Only a few jurisdictions noted having specific requirements for CTPs in this area, while others were considering appropriate rules. Requirements in place or being considered typically relate to the establishment of system control frameworks designed to maintain a high degree of reliability, availability and security, as well as business continuity requirements.

*(j) Cyber Security*

As with responses related to system resiliency, integrity and security, many jurisdictions viewed the nature of cyber security risks for CTPs to be like those applicable to Trading Venues. Some however, did identify concerns related to unique risks of CTPs and/or inherent in the use of the underlying technology.

Where participant assets are custodied by the CTP (especially where assets are stored in hot wallets), some jurisdictions indicated that there is an increased risk of cyber attack and conveyed a lack of certainty that CTPs are sufficiently equipped to repel such attacks. Others expressed concerns over poorly-programmed smart contracts and a lack of clarity around details when an attack has occurred.

Only a few jurisdictions noted having specific requirements for CTPs in this area, while others were considering appropriate rules. Requirements in place or being considered typically relate to the establishment of control frameworks and/or adherence to cyber security standards.

### *(k) Clearing and Settlement*

Some respondents indicated that counterparty risk is important in relation to clearing and settlement for CTPs. The execution of orders and the corresponding transfer of ownership may be recorded in the internal ledger of the CTP, but not on the underlying ledger of the asset. These circumstances may raise concerns about counterparty risk that participants assume vis-à-vis the platform.

Other jurisdictions noted that traditional notions of clearing and settlement are not applicable to crypto-assets and that a lack of clarity by CTPs regarding settlement may lead to incorrect assumptions by participants. It was also noted that risks regarding settlement may be somewhat mitigated given that trading on CTP's are typically fully-funded.

Several jurisdictions are considering or are in the process of policy development related to clearing and settlement risk of crypto-assets while others have already put in place specific requirements. They include:

- Requirements to establish clear processes for efficient settlement;
- Requiring fully-funded trading to minimize risk of settlement failure;
- Disclosure of delayed settlement (e.g., due to network congestion);
- Clear disclosure of the obligations of the CTP with respect to the delivery of crypto-assets or cash; and
- Requirements related to risk management.

### *(l) Cross-Border Issues*

Respondents noted that crypto-assets are generally global in nature and that it may be difficult to establish or identify the precise location of the operator of a CTP or where the regulated activity is occurring. A CTP may be offering services to participants in any jurisdiction, including where specific activities may be prohibited, and there is likely to be a much higher risk of participants in one jurisdiction using a CTP that is regulated by a different regulatory authority.

There may also be specific risks relating to regulatory arbitrage between jurisdictions. A crypto-asset that is deemed to be a security in one jurisdiction may be unregulated in another and investors may face different legal frameworks and different levels of recourse in the event of an issue. Further, supervisory or law enforcement activities may be challenged due to the cross-border nature of trading.