Provisional Translation

Report by the Working Group on Crypto-asset Systems of the Financial System Council

December 10, 2025

Financial Services Agency

Table of Contents

List of Members of the Working Group on Crypto-asset Systems of the Financial System Council

As of December 10, 2025

Chair	MORISHITA, Tetsuo	Professor, Faculty of Law, Sophia University
Members	ARIYOSHI, Naoya	Partner, Attorney at Law, Nishimura & Asahi (Gaikokuho Kyodo Jigyo)
	ITO, Aki	Partner, Attorney at Law, KATAOKA & KOBAYASHI LPC
	IWASHITA, Naoyuki	Professor, School of Government, Kyoto University
	OTSUKI, Nana	Professor, Business School, Nagoya University of Commerce and Business
	OGAWA, Keiko	Partner, CPA, Financial Services Global Accounts Leader, EY Strategy and Consulting Co., Ltd.
	KATO, Takahito	Professor, Graduate Schools for Law and Politics, The University of Tokyo
	KAWAMURA, Kenji	Professor, Department of Law, Rikkyo University
	KONO, Yasuko	Director, Japan Consumer's Association
	SAKO, Kazue	Professor, Faculty of Science and Engineering, Waseda University
	NAGASAWA, Yumiko	Founder & Organizer, Association for Fostering Quality Financial Product
	MATSUI, Tomoyo	Professor, Graduate Schools for Law and Politics, The University of Tokyo
	MATSUO, Ken'ichi	Professor, Graduate School of Law, Kyoto University
	MATSUO, Shin'ichiro	Research Professor of Computer Science, Georgetown University / Research Professor, Virginia Polytechnic Institute and State University

(Honorifics omitted, in *Gojuon* (Japanese alphabet) order)

Observers
- Japan Virtual and Crypto assets Exchange Association
- Japanese Bankers Association
- International Bankers Association
- Trust Companies Association of Japan
- Japan Securities Dealers Association
- The Investment Trusts Association, Japan
- Japan Investment Advisers Association
- The Financial Futures Association of Japan
- Type II Financial Instruments Firms Association
- Japan Security Token Association
- Financial Instruments Mediation Assistance Center
- Japan Cryptoasset Business Association
- Japan Blockchain Association
- Fintech Association of Japan
- National Police Agency
- Consumer Affairs Agency
- Digital Agency
- Ministry of Justice
- Ministry of Finance

I. Introduction

1. Development of the Legal and Regulatory Framework for Crypto-Assets

In Japan, in response to international calls to strengthen anti-money laundering and counter-terrorist financing (AML/CFT) measures,[1] [2] as well as domestic failures involving a business operator engaged in the exchange of crypto-assets and legal tender, the Payment Services Act (hereinafter, the "PSA") and related laws were amended in 2016, thereby introducing one of the world's first regulatory frameworks for crypto-assets (then referred to as "virtual currencies"). These amendments established a registration regime for business operators engaged in the exchange of crypto-assets and legal tender and introduced a user protection framework, including AML/CFT measures such as customer[3] due diligence at account opening, obligations to provide explanations to users, and requirements to segregate users' assets (effective April 2017).

Subsequently, in light of various issues that had been identified—including inadequate internal control systems at crypto-asset exchange service providers (hereinafter, "CASPs"), incidents involving the outflow or misappropriation of crypto-assets and legal tender entrusted by users, and excessive advertising—the PSA, the Financial Instruments and Exchange Act (hereinafter, the "FIEA"), and related laws were amended in 2019 (effective May 2020).[4] These amendments changed the notification requirement for changes to crypto-assets handled by CASPs from ex post notification to prior notification, introduced regulations on advertising and solicitation, and, in principle, required CASPs to manage users' crypto-assets in cold wallets.[5] In addition, in response to new types of

---

[1] In the G7 Elmau Summit Leaders' Declaration (June 2015), the leaders agreed as follows: "We will take further actions to ensure greater transparency of all financial flows, including through appropriate regulation of virtual currencies and other new payment methods."

[2] The FATF's Guidance "Guidance for a Risk-Based Approach to Virtual Currencies" (June 2015) states, in essence, that countries should require exchanges between virtual currencies and fiat currencies to be registered or licensed and subject them to AML/CFT requirements, including customer due diligence obligations.

[3] When referring to persons who trade crypto-assets, this report generally uses the term "user." This reflects the view that the term "investor" may not be appropriate, given the presence of speculative trading and the fact that crypto-assets may also be used for payment purposes. The term "investor" is therefore used only in widely used expressions such as "individual investor" and "retail investor."

[4] Under the same amendment, the statutory term was changed from "virtual currency" to "crypto-assets."

[5] This refers to a method of managing signature keys and other information necessary for transferring

transactions and unfair practices involving crypto-assets, a regulatory framework for crypto-asset derivatives was established; it was clarified that ICO (Initial Coin Offering) tokens conferring rights to receive profit distributions fall within the scope of the FIEA; and market abuse regulations, including prohibitions on market manipulation involving crypto-assets, were also introduced.

Furthermore, in 2022, following the recommendations of the Financial Action Task Force (hereinafter, "FATF"), the Act on Prevention of Transfer of Criminal Proceeds (hereinafter, the "APTCP") and related laws were amended (effective June 2023) to introduce the so-called Travel Rule.[6] Under this rule, when a CASP transfers crypto-assets at a user's request, it must provide the receiving CASP with information identifying both the originator and the beneficiary.

Most recently, in June 2025, the PSA was amended to introduce measures including authorizing the authorities to issue orders requiring CASPs and related entities to retain assets within Japan, in order to prevent the outflow of assets overseas in the event of their failure, and establishing a new category of intermediary business engaged solely in brokering the purchases, sale, or exchange of crypto-assets (scheduled to come into force within one year of promulgation).

2. Review in Light of the Increasing Recognition of Crypto-Assets as Investment Targets

While Japan has progressively developed regulatory frameworks to enhance user protection and AML/CFT measures, the Financial Services Agency (FSA), in light of technological developments and changes in the environment surrounding crypto-assets, examined the appropriate regulatory framework for crypto-assets and published its findings in a discussion paper on April 10, 2025.[7] The paper noted that crypto-assets have increasingly been regarded as investment targets by users in Japan and abroad, and that fraudulent investment solicitations have emerged, thereby highlighting the need to further strengthen the framework for user protection. The general direction set out in the

crypto-assets by recording and storing them on electronic devices that are not constantly connected to the internet, or through other technologically equivalent security measures. While the FSA's Supervisory Guidelines, Volume III: Financial Companies use the term "secret key," it has been pointed out that the term "signature key" is more consistent with ISO/IEC 14888. Accordingly, this report uses the term "signature key."

[6] In 2022, the Payment Services Act was amended to establish a regulatory framework for so-called stablecoins, with the amendment taking effect in June 2023.

[7] Discussion Paper: "Examination of the Regulatory Systems Related to Crypto-Assets"
< https://www.fsa.go.jp/en/news/2025/20250410_2/crypto_dp.html> (English version)
<https://www.fsa.go.jp/news/r6/sonota/20250410_2/01.pdf>

discussion paper received broad support in the public comments submitted in response.[8]

Against this backdrop, at the joint session of the 55th General Meeting of the Financial System Council and the 43rd Meeting of the Sectional Committee on the Financial System, held on June 25, 2025, the Minister of State for Financial Services requested that, “In light of the increasing recognition of crypto-assets as investment targets by domestic and foreign investors alike, the Council examine the appropriate regulatory framework for crypto-assets, while giving due consideration to both user protection and the promotion of innovation.” In response, the Financial System Council established the Working Group on Crypto-Asset Systems (hereinafter, the "Working Group"), which held six meetings beginning in July 2025 to deliberate on the appropriate regulatory framework for crypto-assets. This report summarizes the outcome of those deliberations.

8 Summary of Comments: <https://www.fsa.go.jp/news/r7/sonota/20250731_2/01.pdf>

II. Current Status and Challenges of Crypto-Asset Transactions

1. Current Status of Crypto-Asset Transactions

Crypto-assets are forms of economic value that can be transferred over the internet using blockchain technology. Their characteristics vary widely depending on factors such as transaction validation methods, whether there is a centralized controlling entity, and whether they provide utility in connection with specific projects.

Currently, under the PSA, crypto-assets are regulated primarily as payment instruments, including through rules governing transactions with users and the custody of crypto-assets. Recent developments indicate that the number of accounts opened with domestic CASPs exceeds 13 million and that user deposits exceed JPY 5 trillion[9] (both figures as of October 2025). In addition, approximately 70 percent of crypto-asset holders fall into income brackets below JPY 7 million,[10] and more than 80 percent of individual accounts hold assets of less than JPY 0.1 million;[11] accordingly, crypto-asset ownership has become increasingly widespread among retail users.

Against this backdrop, although crypto-assets continue to be used to some extent as a means of payment, their role as investment targets has been expanding both domestically and internationally, as outlined below.[12]

- According to a domestic survey of individual investors, the proportion of crypto-asset holders among those with investment experience (7.3 percent) exceeds the proportions of FX traders and corporate bond investors.[13] Moreover, the predominant reason for holding crypto-assets (86.6 percent) is the expectation of long-term price appreciation.[14]

- Internationally, exchange-traded funds (ETFs) linked to the prices of crypto-assets such as Bitcoin

---

9 Source: Japan Virtual and Crypto assets Exchange Association (JVCEA), "Members' Crypto-Asset Trading Status (Monthly)" (updated December 3, 2025)

10 Source: Japan Cryptoasset Business Association, "Survey Results on Tax Filing for Crypto-Assets and Proposals for Tax Reform"

11 Source: JVCEA, "Annual Report on Crypto-Asset Trading, FY2024"

12 Some argued that allocating funds to such crypto-assets should be described as "speculation" rather than "investment." However, this report uses the term "investment" to mean "generally, allocating capital for the purpose of earning a profit" (Yuhikaku, Yuhikaku Legal Terminology Dictionary, 5th ed.).

13 Source: FSA, "the Results of the Awareness Survey of Customers Regarding Risk-Involving Financial Instruments Sales" (July 5, 2024)

14 See footnote 10.

have been listed in many jurisdictions, including the United States and Canada, and capital continues to flow into crypto-assets through these vehicles.

・In the United States, it has been noted that the number of institutional investors investing in Bitcoin ETFs—including pension funds pursuing long-term investment strategies—is increasing, [15] and that crypto-assets are increasingly being recognized as part of diversified investment portfolios.

・Survey results also indicate that, among domestic institutional investors, crypto-assets are viewed as an opportunity for portfolio diversification and that investment appetite is increasing.[16]

On the other hand, the FSA's Financial Services User Consultation Office currently receives, on average, more than 350 crypto-asset-related inquiries and complaints per month,[17] the majority of which concern fraudulent investment solicitations or transactions. In a sense, such issues can be attributed to the growing recognition of crypto-assets as investment targets among the general public. At the same time, this trend underscores the growing need to strengthen user protection.

In addition, crypto-assets have been identified as a means of transferring criminal proceeds, including those derived from organized fraud, and there are concerns that outflows of crypto-assets resulting from cyberattacks on CASPs could be used to finance terrorism.

2. Pressing Challenges

For users to engage in crypto-asset transactions with confidence, it is essential to ensure both an appropriate trading environment and effective user protection. As crypto-assets are increasingly treated as investment targets, a number of pressing challenges relating to crypto-assets, as outlined below, have emerged. While user-protection frameworks have been developed, further measures are needed to strengthen both user protection and the trading environment.

---

[15] Source: The Nikkei (November 30, 2024)

[16] Source: Nomura Holdings and Laser Digital Holdings AG, "Survey on Digital Asset Investment Trends for Institutional Investors 2024" (June 2024)

[17] For example, during July–September 2025, 1,487 inquiries and consultations related to crypto-assets and similar matters were received, accounting for around 10% of all inquiries and consultations in that category. In addition, the National Consumer Affairs Center of Japan received 7,227 consultations concerning crypto-assets during FY 2024. This exceeds the number of consultations relating to life insurance (4,222) and investment trusts (366) received during the same period.

① Enhancing Disclosure

It has been noted that white papers issued in connection with crypto-assets at the time of issuance often contain unclear descriptions or discrepancies between their stated features and the underlying code. Moreover, such information disclosure has thus far been required only of CASPs under a self-regulatory framework, and concerns have been raised that clear and accurate information is not consistently provided and that comparability across crypto-assets remains limited. Therefore, it is necessary to enhance information disclosure regarding crypto-assets so that users can make informed and rational trading decisions based on accurate information about their functions and value.

② Ensuring Appropriate Transactions and Addressing Unregistered Operators

In recent years, there has been an increase in entities, including those based overseas, soliciting crypto-asset transactions without registration as CASPs (unregistered operators), and the FSA has received numerous inquiries regarding such fraudulent solicitations. Given the high degree of pseudonymity associated with crypto-assets, the difficulty of providing redress once misconduct has occurred, and the need to prevent their use for criminal purposes, stricter regulations are needed to deter unlawful solicitations by unregistered operators.[18]

In addition, given the high volatility of crypto-assets relative to traditional financial instruments, it is necessary to ensure that transactions are conducted in a manner commensurate with users' risk tolerance and financial capacity.

③ Addressing Inappropriate Conduct in Investment Management

Investment seminars related to crypto-asset transactions and online communities claiming to provide information have also emerged; some are suspected of engaging in misconduct, including defrauding users. In light of these circumstances, it is necessary, from the perspective of user protection, to ensure the proper conduct of crypto-asset-related investment management and advisory activities.

④ Ensuring Fairness in Price Formation and Trading

[18] The Government of Japan's Public Relations Office website ("Beware of claims that you will 'definitely make money' with crypto-assets! Problems originating from dating apps and social media are increasing," July 25, 2025) and the Tokyo Metropolitan Consumer Affairs Center website, Tokyo Kurashi Net ("Invited by a friend, I borrowed money and ended up entering into a network-marketing contract for a crypto-asset investment seminar," November-December 2022 issue), also warn consumers about solicitations to investment seminars and online communities, as well as fraud and other harmful schemes involving unknown operators or individuals through dating apps and similar services.

Given the listing of Bitcoin ETFs and similar instruments in overseas markets, as well as growing global investment in crypto-assets by both retail and institutional investors, the need to ensure fairness in the price formation and trading of crypto-assets—which also serve as underlying assets of such instruments—is increasing. In addition, the International Organization of Securities Commissions (IOSCO) has recommended strengthening measures to address fraud and market abuse, including insider trading, in relation to crypto-assets.[19] Moreover, legislative measures to address insider trading have been introduced in the EU[20] and the Republic of Korea,[21] and enforcement actions involving insider trading have been observed in the United States.[22] In light of these developments, the need to strengthen responses to insider trading in crypto-assets is also growing in Japan.

⑤ Strengthening Cybersecurity

Incidents involving the loss of crypto-assets due to cyberattacks on CASPs continue to occur both in Japan and abroad. Attack methods have become increasingly sophisticated, including the use of social engineering, and reliance on cold wallets alone no longer guarantees safety. In some cases, attackers include nation-states seeking to secure funds for terrorism or weapon development. As a result, these threats are difficult for individual companies—particularly start-ups—to address on their own. Accordingly, in addition to government support, cross-industry cooperation through information sharing and analysis has become essential. Against this backdrop, the industry must establish robust cybersecurity management frameworks to prevent Japan's assets from falling into the hands of malicious actors and to safeguard users' interests. CASPs must also appropriately manage risks related to the outflow of users' assets and continuously review their measures in line with technological developments. Maintaining a minimum level of cybersecurity risk management is essential, but it is also important to promote continuous improvements in cybersecurity capabilities across the industry.

---

[19] IOSCO, "Policy Recommendations for Crypto and Digital Asset Markets Final Report" (November 2023)

[20] The Markets in Crypto-Assets Regulation (MiCA).

[21] The Act on the Protection of Virtual Asset Users.

[22] See footnote 95.

III. Required Measures

1. Approaches to Regulatory Revisions

(1) Purpose of the Regulatory Revisions

To address these challenges, the regulatory revisions should aim to strengthen user protection by establishing a framework that treats crypto-assets as financial instruments in a manner that reflects their characteristics, taking into account their growing role as investment targets and the emergence of fraudulent investment solicitations. At the same time, it should be made clear that such regulatory revisions should not be interpreted as an official endorsement of investment in crypto-assets. Rather, a sound trading environment should be established on the premise that users make reasonable trading decisions based on a sufficient understanding of the risks and product characteristics and engage in transactions within their risk tolerance.

Furthermore, the sound development of the digital economy is important for addressing Japan's social challenges and enhancing productivity. Although it is currently difficult to foresee how the crypto-asset markets will evolve, it is also important to support the potential for sound innovation in Japan.

(2) Key Considerations in Revising the Regulatory Framework

In revising the regulatory framework, three key considerations should be emphasized: (i) promoting sound innovation through effective user protection; (ii) taking into account the global nature of crypto-assets, including regulatory developments in other jurisdictions; and (iii) maintaining regulatory flexibility, given the diversity of crypto-assets and the rapid evolution of related technologies and business models. In addition, as crypto-assets may also be used as a means of payment, care should be taken not to unduly restrict their use.

At the same time, while stronger regulation is necessary to address these challenges and ensure user protection, excessive regulatory burdens on service providers should be avoided, as they could undermine user convenience.[23]

In designing an appropriate regulatory framework, it is essential to keep these points in mind and

---

[23] There was a view that the institutional capacity of the self-regulatory organization and related bodies will need to be fundamentally strengthened going forward. At the same time, it was also suggested that, when implementing the revised regulatory framework, priorities should be set and requirements introduced in a phased and proportionate manner.

take full account of the actual state of crypto-assets. Crypto-assets originated, in part, as a means of circumventing traditional financial frameworks. While transactions are recorded on-chain using blockchain technology, a degree of pseudonymity is preserved, and transfers can occur across borders in real time. While holdings by retail users are increasing, crypto-assets have also been identified as a global means of transferring or concealing illicit funds. In Japan, retail transactions are engaged primarily off-chain through CASPs, and the proposed regulatory revisions therefore focus on such transactions, where the need for user protection is particularly high.[24] However, these transactions represent only a portion of global crypto-asset trading. For example, while user deposits held by domestic CASPs exceed JPY 5 trillion (as of October 2025),[25] the global market capitalization of crypto-assets exceeds USD 3 trillion.[26] Price formation and liquidity are driven primarily by global trading, including on-chain transactions. While it is important, as far as practicable, to apply the regulatory frameworks used in traditional securities markets to crypto-asset markets in order to promote a fair trading environment, this alone cannot ensure that all crypto-assets and related trading activities are sound. It should be recognized that certain aspects of crypto-assets inherently fall beyond the scope of regulation. Accordingly, continued international cooperation among regulatory authorities will be essential.

2. Change of Legal Basis

(1) Use of the FIEA Framework

The pressing challenges surrounding crypto-assets described above closely align with issues that the FIEA has traditionally addressed.

For example, to address information asymmetry between securities issuers and investors, the Act imposes disclosure requirements on issuers in connection with public offerings and secondary distributions of securities. From the perspective of investor protection, it also establishes a range of business regulations governing solicitation, brokerage and intermediation, investment management, and investment advisory services, while requiring the proper management of customer assets. In addition, the FIEA provides a framework for addressing market abuse in order to ensure fair and

---

[24] Since individual users primarily open accounts with domestic CASPs and conduct transactions on trading platforms provided by those CASPs, there is a strong need to ensure user protection in transactions conducted through them.

[25] See footnote 9.

[26] Source: CoinMarketCap (as of November 30, 2025)

transparent markets and protect investors. Its effectiveness is supported by both criminal penalties and an administrative monetary penalty system. The Securities and Exchange Surveillance Commission (hereinafter, the "SESC") plays a central role in enforcement by conducting investigations into criminal violations and seeking measures such as court-issued emergency injunctions against unregistered operators.

More fundamentally, the FIEA is founded on the principle of establishing a comprehensive, cross-cutting investor-protection framework that broadly covers financial instruments with strong investment characteristics. The fact that many crypto-asset transactions are conducted in anticipation of gains from price fluctuations is consistent with the concept of "investment characteristics" discussed at the time of the FIEA's enactment in defining the scope of instruments subject to regulation.[27] [28] In

---

[27] Excerpt from the Interim Report of the First Subcommittee of the Financial System Council's Sectional Committee on Financial System (July 7, 2005).

Under the Investment Services Law, (omitted), the scope of regulation should cover as broad a range of financial instruments as possible.

With respect to the financial instruments covered by the Investment Services Law (hereinafter referred to as "investment instruments"), it is considered appropriate to establish criteria such as the following: (i) the contribution of money and possibility of repayment or redemption; (ii) linkage to assets or an index; and (iii) the assumption of risk in expectation of higher returns (economic utility).

At the same time, when specifically defining investment instruments, it is considered appropriate, from the perspective of investor protection, to enumerate eligible products as broadly as possible, while allowing the authorities to designate products or provide tailored exemptions in light of actual market conditions and developments in the financial environment.

While positioning the Investment Services Law as a general law governing the sale of financial instruments and asset management, (omitted), it would be appropriate, to the fullest extent possible, to integrate into it other laws with similar characteristics.

[28] Toward Legislation for the Investment Services Law (Provisional Title): Excerpt from the Report of the First Subcommittee of the Financial System Council (December 22, 2005).

It is necessary to review the existing sectional laws governing investment and securities businesses and to establish a legal framework that covers a broad range of financial products. The Investment Services Law should be positioned as a general law governing the sale of financial products and asset management, and the same conduct regulations should apply to financial instruments that perform equivalent economic functions, regardless of the type of business.

The criteria in items (i) to (iii) set out in the Interim Summary should form the basis for detailed consideration of the scope of investment instruments subject to regulation under the Investment Services Law, as indicators of whether an instrument has investment characteristics.

In this context, although various interpretations of "risk" and "return" in item (iii) are possible, "risk" may light of these considerations, applying the FIEA framework to crypto-assets is an appropriate means of addressing the challenges identified above.

At the same time, while other products, such as gold or trading cards, may have investment characteristics, not all such products should necessarily fall within the scope of the FIEA.[29] Because regulation entails various costs, it is justified only where the expected benefits outweigh those costs. Accordingly, policymaking should be based on necessity and proportionality, in line with the purpose of the FIEA—namely, "the sound development of the national economy and the protection of investors."

From this perspective, taking comprehensive account of the actual conditions of investment-related transactions involving crypto-assets, the occurrence of investor harm, and their relationship with policies outside the FIEA—such as industrial and resource policies—it is considered that crypto-assets differ from products such as gold or trading cards in terms of the necessity and appropriateness of applying the FIEA regulatory framework.[30]

(2) Positioning of Crypto-Assets under the FIEA

Under the FIEA, "securities" are instruments that represent legal rights entitling their holders to receive distributions, such as dividends or interest. In this respect, crypto-assets generally do not represent such legal rights, nor do they entitle holders to profit distributions or residual asset distributions. Accordingly, crypto-assets differ in nature from securities under the FIEA. It is therefore appropriate to position crypto-assets as a regulated instrument distinct from securities.

(3) Scope of Crypto-Assets under the FIEA

With regard to the scope of crypto-assets to be regulated under the FIEA, it is appropriate to adopt the current legal definition of crypto-assets, taking into account the following considerations:

---

be understood primarily as the presence of market risk or credit risk. "Return," in turn, may be understood primarily as the expectation of monetary profit (positive cash flow), given that such expectations typically underpin users' engagement with investment instruments.

[29] In considering the scope of regulation under the FIEA, relevant criteria may include: (i) whether an instrument constitutes a financial instrument; (ii) whether it has strong investment characteristics; and (iii) the necessity of applying the FIEA, that is, consistency with the purpose of the Act, and the appropriateness of doing so, including from a cost–benefit perspective. It was noted, for example, that gold and trading cards may not satisfy criterion (i) in the first place.

[30] With respect to physical gold and trading cards, given that their practical uses and the limited prevalence of investment-related harm, the necessity and appropriateness of regulating them under the FIEA are currently considered to be low.

・Tokens that do not fall within the definition of crypto-assets under the PSA—so-called NFTs (non-fungible tokens)—often involve the provision of goods or services in practice, and their characteristics vary widely; therefore, whether they should be made uniformly subject to financial regulation requires careful consideration.[31]

・So-called stablecoins (digital-money type) are regulated under the PSA as electronic payment instruments on the premise that they are issued at prices linked to fiat currency and are redeemable at the same amount as the issue price, or its equivalent. While they may be widely used as means of transfer and payment, they are not currently generally regarded as investment targets.

(4) Regulation of Crypto-Assets under the PSA

The regulatory framework applicable to financial instruments business under the FIEA already incorporates requirements comparable to those imposed on crypto-asset exchange services under the PSA. Moreover, with respect to specific requirements under current law—such as security and risk management measures reflecting the high risk of unauthorized outflows of crypto-assets—equivalent provisions can be established under the FIEA, thereby creating a comprehensive regulatory framework for crypto-assets within that Act. Accordingly, to avoid regulatory complexity, it would be appropriate to remove the crypto-asset-related provisions from the PSA.

Furthermore, bringing crypto-assets within the scope of the FIEA would not restrict their use for payment purposes. As is currently the case under the PSA, crypto-assets are widely traded for investment purposes. Strengthening user protection and enforcement through the proposed regulatory revisions would contribute to a more secure trading environment, enabling users—including those who use crypto-assets for payment purposes—to engage in transactions with confidence.

3. Information Disclosure Regulations

Crypto-asset transactions conducted by users are similar in nature to securities transactions. These transactions include both the initial offering of crypto-assets and the trading of crypto-assets already in circulation. In both cases, it is essential that users are provided with the information necessary to make informed trading decisions. Accordingly, as described below, appropriate information should be

[31] NFTs are primarily used in digital content, such as games and art, and their use has also expanded into emerging areas, including ticketing and domain names.

disclosed to users not only at the time of commencement of handling but also on an ongoing basis.[32]

(1) Information Disclosure upon commencement of handling

A. Information Asymmetry Regarding Crypto-Assets

Users face information asymmetry with respect to crypto-assets primarily in the following respects.

(i) The Technical Nature and Expertise of Crypto-Assets

For many users, even where the code governing a crypto-asset's mechanisms is publicly available, such code is difficult to understand. In addition, even when a white paper explaining a crypto-asset's design and mechanisms has been prepared and disclosed, it remains difficult to verify those explanations against the underlying code. Accordingly, given the technical complexity involved and the specialized expertise required, information asymmetry exists between retail users and experts with advanced knowledge of crypto-asset technology.

(ii) Substantive Control over the Sources of Crypto-Asset Value

Where an entity substantively controls the sources of a crypto-asset's value[33] (a centralized controlling entity), the value of the crypto-asset may fluctuate depending on that entity's activities. In such cases, information asymmetry arises between the centralized controlling entity and users.

(iii) Circulation and Holding Status of Crypto-Assets

With respect to the circulation and distribution of crypto-assets, it is difficult for parties other than those engaged in transactions to obtain accurate information. As a result, information asymmetry also exists between those who trade or hold crypto-assets and other market participants.

B. Information to be Disclosed

(i) Addressing Information Asymmetry

To address information asymmetry arising from the technical complexity and specialized expertise associated with crypto-assets, information material to users' trading decisions—such as the characteristics and functionality of the crypto-asset, total number of the crypto-assets, underlying technology, rights and obligations attached to the crypto-assets, and associated risks—should be

---

[32] For an overview of the regulations on information disclosure, see Section V, Reference Material 1.

[33] The value of a crypto-asset may fluctuate depending on factors such as its characteristics and functions, the design of its issuance and supply, and the operation of the underlying project. A relevant party is a person or entity that has the authority to create or modify, at its own discretion, elements that are material to the crypto-asset's value.

disclosed to users in a clear and understandable manner. In addition, where a centralized controlling entity exists (i.e., in the case of crypto-assets with an identifiable issuer), information on that entity—including information about the issuer, the planned use of offering proceeds, the crypto-asset project, and the holding status of the crypto-assets—should also be disclosed to users, in addition to the information described above.

On the other hand, imposing disclosure requirements on large-volume holders to address information asymmetry relating to the circulation and holding status of crypto-assets would present challenges in ensuring the effectiveness of such requirements, particularly with respect to persons engaging in transactions overseas. Furthermore, such regulations have not been adopted in Europe or the United States, and large-volume holdings do not necessarily correspond to substantive control over the sources of value. Accordingly, careful consideration should be given at this stage to whether to impose any such obligation.[34]

Nevertheless, with respect to centralized controlling entities of crypto-assets, it may be appropriate, within the framework of disclosure requirements, to require disclosure of the holding status of the entity and its related parties, as well as information relating to large-scale issuance without consideration.

In addition, for crypto-assets known for their high degree of pseudonymity, it is important to enhance transparency regarding their circulation and holding status. Measures to this end should continue to be considered, taking into account developments in regulatory frameworks overseas.[35]

(ii) Risks and Product Characteristics

To enable users to fully understand the risks and characteristics of crypto-assets and to conduct transactions within their risk tolerance, it is important to disclose information on the risks and characteristics of each crypto-asset in a clear and accessible manner.

With respect to risks associated with crypto-assets, certain risks—such as fraud and significant price volatility—should be addressed through user awareness initiatives and explanations provided by

---

[34] Under the insider trading regulation framework for crypto-assets described below, a person related to a large-volume trader who becomes aware of material facts concerning such trades would generally be prohibited from engaging in transactions involving crypto-assets handled by domestic CASPs, before such information is made public.

[35] For example, from the perspective of addressing money laundering and related risks, it may be appropriate to consider measures in the future to enhance traceability in cases involving large-volume crypto-asset transactions. In doing so, consistency with the revised regulatory framework under the FIEA should also be considered.

CASPs.[36] At the same time, the following types of information relate to risks specific to individual crypto-assets and, given the presence of information asymmetry, should be disclosed directly to users:

- Market capitalization and circulation supply (liquidity risk)
- The number of tokens issued to date, the maximum supply and whether it can be modified; historical issuance and burning records, planned issuance and burnings; and the holdings of the centralized controlling entity and its related parties (dilution risk)
- Information on the centralized controlling entity, the use and status of funds raised, the business plan for the relevant project, and the progress of that project (business risk)
- Mechanisms for validating value transfers, and information related to code audits and security audits (technical and operational risk)

With respect to product characteristics, information such as a crypto-asset's development history, technology, tokenomics, and utility should be disclosed to enable users to understand its features.[37] At the same time, from the perspective of reducing information asymmetry, the specific scope of information to be disclosed—including factors that differentiate[38] a crypto-asset from others, in terms of both advantages and disadvantages—should be examined in practice and reviewed flexibly as necessary.

Finally, for key information on these risks and product characteristics, it may be appropriate to require the provision of summary information to enhance user understanding and improve comparability.

C. Entities subject to Disclosure Requirements

(i) Basic Concept

---

[36] In addition, crypto-assets differ from traditional financial instruments such as stocks and bonds in that they generally lack backing by underlying asset, do not provide dividends or interest, and do not confer shareholder rights. It is important to address these characteristics by raising user awareness and ensuring that CASPs provide appropriate explanations.

[37] Key information to be disclosed may include: the background to the creation of the crypto-asset and its initial development team; the transaction validation process and consensus mechanism; the methods and processes of token issuance, including staking and mining, and token burning; and information on use cases and associated rights and obligations.

[38] It was noted that positive differentiating factors may include information on non-investment use cases and associated rights, while negative differentiating factors may include information such as the reasons for discontinuation by domestic CASPs and any pending litigation.

With respect to entities subject to disclosure requirements, it is necessary to determine who should be required to disclose information from the perspective of addressing information asymmetry. At the same time, in delineating the respective scopes of disclosure requirements and market abuse regulations, the regulatory framework should emphasize clarity while maintaining flexibility, given the rapidly evolving technologies and business models related to crypto-assets.

In this regard, CASPs are in a position to assess various risks, legal compliance, and business feasibility when handling crypto-assets and are therefore expected to possess the necessary technical knowledge and specialized expertise. Accordingly, as a general principle, CASPs that handle crypto-assets should collect the information necessary to address information asymmetry and disclose it to users in a clear and understandable manner.[39]

On the other hand, with respect to crypto-assets with an identifiable issuer, where a centralized controlling entity seeks to raise funds from retail users, that entity should bear primary responsibility for such fundraising and should be required to disclose to users the information necessary to address information asymmetry.[40]

Furthermore, where a domestic CASP independently handles a crypto-asset issued overseas, the CASP may disclose the necessary information, regardless of whether a centralized controlling entity exists. In such cases, given that many domestic users are likely to base their trading decisions on information disclosed by the CASP, consideration should be given to measures to ensure the accuracy and objectivity of that information.

(ii) Criteria for Classifying Crypto-Assets with an Identifiable Issuer

For crypto-assets with an identifiable issuer, risks such as dilution risk and business risk arise from the activities of the centralized controlling entity. It is therefore necessary to address the information asymmetry associated with such risks. Accordingly, it is appropriate to define the scope by focusing on both circulation aspects (authority over issuance and transfer) and substantive aspects (authority over the design and modification of specifications). Under the current framework, crypto-assets falling into any of the following three categories are, in principle, considered to fall within this classification. At the same time, given that new forms of crypto-assets may emerge in the future, the regulatory

---

[39] For crypto-assets that do not have an identifiable issuer, information asymmetry may be greater than for those that have an identifiable issuer. Accordingly, there was a view that further consideration should be given to ensuring that users are provided with information material to their trading decisions.

[40] Even where there is no fundraising by a centralized controlling entity, such an entity may influence price formation by modifying the specifications of a crypto-asset. It has therefore been suggested that such entities could be subject to disclosure obligations.

framework should remain flexible so that determinations can be made in light of the actual circumstances.[41]

- Crypto-assets for which only a specific party has the authority to issue them (i.e., where an entity exists that controls issuance or generation)
- Crypto-assets based on a permissioned blockchain[42] (i.e., where an entity exists that controls transfers)
- Crypto-assets issued based on token standards such as ERC-20[43] (i.e., where an entity exists that defines the specifications)

Under these criteria, it should be possible to determine, in an objective and externally verifiable manner, whether a crypto-asset qualifies as a crypto-asset with an identifiable issuer. Such determination should first be made through a review by the CASP handling the crypto-asset, followed by a review by self-regulatory organizations (hereinafter "SROs").

(iii) Scope of the Centralized Controlling Entity

With respect to the centralized controlling entity of a crypto-asset with an identifiable issuer, the entity that has authority over issuance and transfer and over the design and modification of specifications, and the entity that operates the project associated with the crypto-asset, are ordinarily considered to be the same. Accordingly, in principle, the entity that holds such authorities should be regarded as the centralized controlling entity, including cases in which multiple persons jointly constitute a single entity. In applying this framework, the regulation should be implemented in a manner that prevents regulatory arbitrage. For example, where the entity that holds such authority and the entity that operates the project associated with the crypto-asset are formally separate, they should nevertheless be regarded as a single centralized controlling entity.

D. Activities subject to the Disclosure Requirements

When a centralized controlling entity (an identifiable issuer) raises funds through the sale of crypto-assets, the disclosure requirements should apply not only to the sale of newly generated or issued crypto-assets (primary transactions) but also to fundraising through the sale of crypto-assets that have

---

[41] The framework should be kept under continuous review to ensure that future developments are appropriately captured.

[42] Distributed ledgers can broadly be classified into permissionless ledgers, which impose no restrictions on network participation, and permissioned ledgers, which require permission from an administrator to participate, including private and consortium types.

[43] A standard specification for handling fungible tokens on Ethereum.

already been generated or issued (secondary transactions). However, crypto-assets offered free of charge or tokens automatically granted as rewards should be excluded from the scope of regulation, as they do not constitute fundraising by the issuer.

Moreover, even where the issuer does not raise funds through the sale of crypto-assets, a CASP that handles the relevant crypto-asset should disclose the necessary information as described above. In such cases, in addition to information required to address information asymmetry arising from the technical complexity and specialized expertise, information concerning the issuer should also be disclosed to users. Such information should be based on publicly available sources or information obtained from the issuer, and those sources should be clearly distinguished.

E. Issuer Conduct Equivalent to Private Placements or Private Secondary Distributions

When crypto-assets are solicited for sale to a small number of persons (49 or fewer), those persons are generally considered to have a close relationship with the issuer and are therefore likely to possess sufficient knowledge of the issuer or adequate bargaining power. Similarly, when solicitations are made to professional investors (qualified institutional investors), those investors are recognized under the FIEA as having specialized knowledge and experience in securities investment and as being capable of making appropriate trading decisions. In particular, professional investors are expected to be able to refrain from entering into transactions when they cannot obtain or adequately assess relevant information. This capability is considered to extend not only to securities but also to a wide range of financial instruments, including crypto-assets. Accordingly, it is appropriate to exempt such solicitations from information disclosure requirements.[44]

Furthermore, where CASPs conduct solicitations on behalf of issuers targeting a small number of persons or professional investors, the need for regulatory protection through disclosure requirements is similarly limited. Therefore, it is appropriate to exempt CASPs from disclosure obligations in such cases.

To prevent regulatory circumvention, appropriate transfer restrictions should be imposed. In particular, measures should be taken to prevent tokens solicited or sold to a small number of persons from subsequently being transferred to a large number of persons, and to ensure that crypto-assets

---

[44] Where the amount raised is small, an exemption from disclosure obligations could be considered in light of the costs borne by the issuer. However, it is desirable for information to be disclosed where solicitation is made broadly to retail investors. Moreover, startups' financing needs can be met through frameworks equivalent to small-number private placements and professional private placements, and there is no practical need to exempt small offerings from disclosure requirements. Accordingly, such cases should be subject to disclosure requirements.

solicited or sold to professional investors are not transferred to non-professional investors. Such restrictions may include limiting transfers to a single transferee of the entire holding or restricting transfers exclusively to professional investors. In addition, persons intending to conduct resales should be required to notify counterparties of the existence of such transfer restrictions.

On the other hand, when issuers broadly raise funds from retail investors through a CASP, or when a CASP decides to handle crypto-assets on a "trading platform" or "sales platform",[45] information necessary for trading decisions should be made available to retail investors by either the issuer or the CASP. In such cases, transfer restrictions should be lifted, and resales to retail investors should be permitted.

F. Regulations on Crypto-related Businesses Applicable to Issuers

Except in cases equivalent to private placements or private secondary distributions, an issuer's sale of crypto-assets should continue to require CASP registration, in order to prevent the fraudulent offerings seen in ICOs. Where the issuer entrusts the handling of such sales to a CASP, the issuer should not be required to register as a CASP.[46]

G. Methods and Timing of Information Disclosure

Information prepared by the issuer should be made publicly available on the issuer's website before any solicitation of users. In addition, CASPs handling the relevant crypto-asset should be required to publish such information on their websites and disclose it to customers. Similarly, information prepared by CASPs should be made publicly available on their websites before any solicitation of customers, and CASPs should be required to disclose such information to customers. Furthermore, to ensure ease of access and consistency, information disclosed or provided by issuers and CASPs should also be made available on SRO websites.

In addition, where a crypto-asset with an identifiable issuer is "listed" on a CASP without the issuer's involvement, measures are needed to prevent the issuer from avoiding disclosing information while effectively raising funds. In the case of a "sales platform", CASPs should investigate and confirm that the counterparty supplying the crypto-asset is not the issuer; in the case of a "trading platform," CASPs should investigate and confirm that the customer seeking to sell the crypto-asset is not the issuer.

---

[45] Among the platforms provided by CASPs, those on which customers trade crypto-assets with the CASP acting as principal are generally referred to as "sales platforms," while those on which orders are matched between customers are referred to as "trading platforms." For convenience, this report uses "sales platforms" for the former and "trading platforms" for the latter.

[46] For the relationship between disclosure requirements and crypto-related business regulations, see Section V, Reference Material 2.

Where a sale is determined to constitute fundraising by the issuer, the CASP should be required to refuse the transaction.

(2) Ongoing Disclosure Requirements

A. Timely Disclosure

Information disclosed upon commencement of handling may lose its usefulness for trading decisions over time. To address information asymmetry after the commencement of handling and to enable users to make reasonable trading decisions in the secondary market, ongoing disclosure is indispensable.

In particular, because crypto-assets often involve technologies and specifications that are still under development, the pace of change is expected to be faster than for traditional financial instruments. Therefore, it is particularly important that appropriate information be disclosed in a timely manner, in light of prevailing circumstances.

Accordingly, when an event occurs that may have a significant impact on trading decisions, the issuer or the CASP that disclosed the information at the time of initial listing should be required to disclose timely information to users.[47] Where such events result in changes to the content of the summary information, the summary should also be updated promptly. Furthermore, what constitutes an event that may significantly affect trading decisions should be examined in practice with a view to ensuring sufficient clarity.

B. Periodic Disclosure

With respect to crypto-assets, as noted above, the timely disclosure of information is of primary importance, and the need for periodic disclosure is relatively limited. In this regard, since information prepared and disclosed by CASPs is, in principle, based on publicly available information concerning the crypto-asset, there is limited need to require CASPs, as a statutory obligation, to periodically compile and present such information.[48] On the other hand, with respect to the issuer's business

---

[47] To avoid imposing an excessive burden on CASPs handling a large number of crypto-assets, it was suggested that priority be given to crypto-assets with higher trading volumes. For crypto-assets with lower trading volumes, CASPs could instead warn users that the timeliness and accuracy of the disclosed information may be limited.

In addition, from the perspectives of user protection and reducing the burden on CASPs, it was suggested that, where multiple CASPs handle the same crypto-asset, consideration should be given to establishing, through an SRO, a framework for standardized and consolidated disclosure, in addition to ensuring that information can be viewed in an integrated manner.

[48] Nevertheless, the periodic disclosure of consolidated, regularly updated, and easily accessible

activities—including information concerning the issuer, the use of offering proceeds, the progress of the relevant project, and the holdings of the issuer and its related parties—it may be appropriate, from the perspective of user convenience, to require the issuer, which bears the obligation of timely disclosure, to also make periodic disclosure as a complement to timely disclosure, thereby enabling users to readily grasp the overall picture of the issuer's most recent activities. With respect to the frequency of periodic disclosure, given that such disclosure is intended only to complement timely disclosure and that annual reporting is the general standard under the Companies Act and the FIEA, it is appropriate to require periodic disclosure on an annual basis.[49]

C. Methods of Ongoing Disclosure

Information prepared by the issuer on a timely or periodic basis should be made publicly available on the issuer's website and on the website of CASPs that handle the relevant crypto-asset.

Similarly, CASPs should make timely information publicly available on their websites. In this regard, it is undesirable for timely information concerning the same crypto-asset to be prepared or disclosed with differing content or at different times across CASPs. Therefore, due regard should be given to timeliness, and coordination with SROs should be ensured.

Information publicly disclosed or provided by issuers and CASPs should also be made available on SRO websites so that users can access it in a consolidated manner. In addition, to enable users to access such information easily, it should be organized and presented clearly in chronological order on websites. Furthermore, to ensure comparability, the format for disclosing information should be standardized to the extent possible. Looking ahead, systems that enable access to such information through APIs are expected to be developed.

D. Termination of, or Exemption from, Ongoing Disclosure Obligations

(i) Termination of the Issuer's Ongoing Disclosure Obligations

Where a crypto-asset initially has an identifiable issuer (a centralized controlling entity), but that entity's activities subsequently cease to be material to users' trading decisions—for example, as a result of decentralization—it may be appropriate to allow the competent authority to approve the termination of the issuer's ongoing disclosure obligations. However, even in such cases, information asymmetry

information on crypto-assets would enhance user convenience; accordingly, regular updates under a self-regulatory framework may be considered.

[49] Given that there is currently no settled view regarding the content of information to be disclosed periodically, it has been suggested that, as an initial approach, the content and frequency of disclosure to be determined under a self-regulatory framework according to the type of crypto-asset.

arising from the technical complexity of crypto-assets and the specialized expertise required to understand them may persist. Accordingly, CASPs should remain subject to ongoing disclosure obligations.[50]

If the crypto-asset subsequently becomes subject again to centralized control and the relevant entity resumes fundraising through the sale of the crypto-asset, the issuer should again be made subject to ongoing disclosure obligations.

(ii) Exemption of the Issuer from Ongoing Disclosure Obligations

Where all domestic CASPs delist a particular crypto-asset, and the absence of such information would not adversely affect the public interest or user protection, the need for ongoing disclosure may diminish. In such circumstances, it may be appropriate for the competent authority to exempt the issuer from its ongoing disclosure obligations.

(iii) Exemption of the CASP from Ongoing Disclosure Obligations

Where a CASP delists a crypto-asset, it may be appropriate to exempt the CASP from ongoing disclosure obligations, provided that it gives customers sufficient prior notice of the discontinuation of handling.[51]

(3) Ensuring the accuracy and objectivity of the information disclosed, and user protection at the time of offerings and secondary distributions

A. Ensuring the Accuracy and Objectivity of the Information Disclosed

To enable users to engage in crypto-asset transactions on the basis of appropriate trading decisions, it is essential to disclose accurate and reliable information to address information asymmetry. This includes both information disclosed upon commencement of handling and information disclosed on an ongoing basis. From this perspective, measures should be considered to ensure the accuracy and objectivity of such information, in particular the following:

・The establishment of a regulatory framework governing parties subject to disclosure obligations

・The strengthening of review mechanisms for information prepared

---

[50] In granting approval, appropriate measures should be taken to ensure that, even after the issuer's ongoing disclosure obligations have been lifted, access to necessary information does not become more difficult.

[51] It has been suggested that, when a CASP ceases to handle a crypto-asset, due consideration should be given to users holding that crypto-asset.

Furthermore, taking into account future developments in market practices and the evolution of relevant business models, the use of third-party assessments should also be considered.

(i) Regulatory Framework Governing Parties Subject to Disclosure Obligations

With respect to material misstatements or omissions to disclose information by issuers, it is, in principle, appropriate to impose sanctions on issuers and to provide for civil liability for damages, in a manner similar to that applicable to material misstatements in, or omissions to file, securities registration statements.[52] [53] In addition, where a CASP handles a crypto-asset despite knowing that material misstatements or omissions exist or that information prepared by the issuer has not been disclosed, it may also be appropriate to impose sanctions on the CASP.[54]

Furthermore, because information prepared by CASPs is generally based on publicly available information, and users can obtain such information independently if they have sufficient capacity to do so, sanctions for material misstatements or omissions by CASPs to disclose information should be less severe than those applicable to issuers. With respect to civil liability for damages, for example, it may be appropriate to provide only for statutory damages or presumptions of damages, taking into account the difficulty of proving actual damages.

In addition to the foregoing, where material misstatements occur or required information is not disclosed by issuers or CASPs—or where a CASP handles a crypto-asset despite being aware of such deficiencies—the introduction of an administrative monetary penalty system applicable to both issuers and CASPs should also be considered. Moreover, in cases involving material misstatements or omissions, measures should be established to enable the suspension of trading in the relevant crypto-asset across all domestic CASPs.[55]

---

[52] For misstatements in securities registration statements and annual securities reports, the penalties include imprisonment for up to 10 years, a fine of up to 10 million yen, or both. For failure to file securities registration statements or annual securities reports, the penalties include imprisonment for up to 5 years, a fine of up to 5 million yen, or both.

[53] For misstatements in securities registration statements, the issuer is subject to liability without fault, and the amount of damages is prescribed by statute. For false statements in annual securities reports, the issuer is subject to negligence-based liability with a reversed burden of proof, and the amount of damages is statutorily presumed.

[54] Given that, with respect to extraordinary reports concerning securities, measures to ensure the accuracy of disclosures apply only to issuers, a similar approach may be adopted for misstatements in timely disclosures.

[55] Even in such cases, from the standpoint of user protection, users should be allowed to transfer the relevant crypto-assets out of their wallets even after handling has been suspended.

(ii) Strengthening the Review of Prepared Information

The following measures should be implemented to strengthen the review functions of CASPs and SROs:[56]

- The statutory imposition of review obligations on CASPs, together with the development of appropriate organizational frameworks to support such reviews
- The requirement for code audits[57] [58] to be conducted by technically qualified third parties, as well as for consultation with SROs during CASP reviews
- The establishment within SROs of independent committees or organizations, and the centralization of review functions, in order to enhance the neutrality and independence of such reviews
- Allowing SROs to outsource part of their review functions to third parties with specialized expertise

B. User Protection in Offerings and Secondary Distributions

With respect to offerings and secondary distributions of crypto-assets, it has been pointed out that the issuer's primary objective is fundraising and that their economic incentives to meet users' expectations after fundraising may be limited. For example, in some cases, prices have declined sharply following offerings and secondary distributions in connection with fundraising through the sale of crypto-assets via CASPs (IEOs, or Initial Exchange Offerings). While SROs are currently considering measures to address these issues, structural challenges of this nature cannot be resolved solely through the disclosure requirements described above and therefore require ongoing efforts. Against this backdrop, as an immediate measure, and while recognizing that transactions undertaken by users with an understanding of the risks are, in principle, their own responsibility, it may be appropriate to strengthen user protection as follows.

(i) Setting Investment Limits

---

[56] To implement these measures, it is considered necessary for the SROs to substantially strengthen their institutional frameworks, as outlined in Section V, Reference Material 5.

[57] To ensure the quality of code audits, it is appropriate for laws, regulations, and guidelines to establish requirements concerning the expertise and organizational frameworks of the entities conducting such audits.

[58] It has been suggested that the basic policies regarding the scope, covered tokens, and criteria for code audits should be clarified to the extent possible, taking into account feasibility and international consistency.

Where offerings and secondary distributions of crypto-assets involve risks relating to the underlying project, it is, in principle, desirable for an audit firm to conduct a financial audit of the issuer's financial condition. Where such audits are not conducted and users are subjected to pressure to invest,[59] additional user protection measures are necessary to ensure that users do not engage in excessive transactions hastily. Therefore, where an issuer raises funds broadly from retail investors without such audits, it may be appropriate, by analogy to equity crowdfunding, for which such audits are not mandatory,[60] to set investment limits in order to prevent users from bearing excessive losses due to pressure to invest.

Furthermore, to prevent users from purchasing crypto-assets in excess of such limits, the contractual arrangements between the issuer and the CASP should provide that the issuer, including business operators deemed to be effectively within the same group, must not conduct multiple fundraising activities simultaneously in Japan.

By contrast, once offerings and secondary distributions of crypto-assets have been completed, the same degree of pressure to invest is generally absent. Therefore, even where financial audits by an audit firm are not conducted, there is no need to impose investment limits. However, appropriate information should be disclosed to ensure that users fully understand the relevant risks, including the absence of financial audits, and conduct transactions within their financial means. In this regard, user protection should be ensured through explanations provided by CASPs and assessments of customer suitability.

(ii) Prevention of Conflicts of Interest at CASPs

Where a CASP has a capital relationship with the issuer or other relevant interests, such as holdings of the relevant crypto-asset, it is important that such conflicts of interest be clearly disclosed to users. This is necessary both to mitigate potential conflicts of interest between the CASP and its users and to ensure that users are able to make informed trading decisions based on a proper understanding of such risks. In addition, on "sales platforms," where the CASP itself acts as the counterparty to customers' transactions, appropriate conflict-of-interest management should be implemented to

---

[59] Since the offering period and secondary distribution period are limited, and allocations may be small due to lotteries or similar mechanisms, there is a risk that users' ability to make careful and appropriate trading decisions may be impaired.

[60] For equity crowdfunding investors (excluding professional investors), the investment limit is the greater of: (i) 5% of net assets (excluding residential real estate), (ii) 5% of annual income, or (iii) JPY500,000, subject to a cap of JPY 2 million where the calculated amount exceeds JPY 2 million. In addition, the requirements for professional investors should be considered in light of the decision-making capacity and risk tolerance required for crypto-asset trading.

protect customers.

(iii) Measures Against Free of Charge Issuances

To ensure that the interests of existing users are not adversely affected by large-scale preferential issuances of crypto-assets to specific persons, contractual arrangements between the issuer and the CASP should, in principle, prohibit the issuer from conducting such issuances during the period in which the crypto-asset is under examination for listing by the CASP and after the commencement of handling. In addition, to mitigate the risk of insider trading, the issuer and its related parties should be subject to restrictions on the sale of crypto-assets they hold during a specified period before and after the commencement of handling (the lock-up period).

4. Regulations on Crypto-asset-related Business

(1) Basic Principles

Given that crypto-assets have a degree of tradability comparable to that of security tokens (i.e., tokens representing securities), entities engaged in the business of purchasing and selling crypto-assets should, in principle, be subject to regulations equivalent to those applicable to Type I Financial Instruments Business.[61] Under the FIEA, the relevant regulatory requirements for conducting the business of trading financial instruments are set out in laws and regulations. By contrast, under the current legal framework of the PSA, in some cases, similar requirements applicable to crypto-assets are imposed through self-regulatory rules. Among these requirements, those of general applicability should appropriately be elevated to the level of laws and regulations. At the same time, given the rapid evolution of technologies and business models relating to crypto-assets, it is necessary to strike an appropriate balance between such laws and regulations and self-regulatory rules, which can be updated flexibly in response to changing circumstances. In addition, with respect to provisions under the current PSA that reflect the specific nature of crypto-assets (e.g., safeguarding obligations), it would be appropriate to introduce corresponding requirements under the FIEA, given that the FIEA currently contains no provisions applicable to Type I Financial Instruments Business that address such aspects.[62]

---

[61] As noted in 3(1)(F), except in cases equivalent to private placements or private secondary distributions, an issuer's sale of its own crypto-assets requires registration as a CASP. The appropriate level of regulation should be considered with reference to the existing FIEA rules governing self-offerings of securities.

[62] For further details on the regulatory approach to business conduct, see Section V, Reference Material 3.

(2) Specific Issues

A. Regulation of Non-core Business Activities

Under the FIEA, the regulations of non-core business activities by Type I Financial Instruments Business are categorized into three types: (i) incidental businesses, (ii) notifiable businesses, and (iii) approved businesses. For activities that do not fall within category (i) or (ii), prior approval from the authority is required to confirm that conducting such businesses would not raise regulatory concerns. With respect to CASPs conducting other businesses, the competent authority should conduct an appropriate prior review from the perspective of preventing conflicts of interest and ensuring that users are not adversely affected by risks arising from such businesses.

On the other hand, unlike Type I Financial Instruments Business, crypto-asset exchange services may also attract business operators for whom such services are not their core business.[63] Accordingly, among businesses other than crypto-asset exchange services, those incidental to such services—such as consulting services related to blockchain technology—may be conducted without notification or prior approval. For other types of businesses, it may be appropriate to require prior notification to the competent authority, rather than prior approval.[64]

Furthermore, where a financial instruments business operator (hereinafter referred to as a "FIBO") that does not currently provide crypto-asset exchange services intends to commence such services, it would be appropriate to require an amendment to its registration.

B. Enhancement of Operational Control Frameworks

In addition to the operational control frameworks already required of CASPs under current laws and regulations—such as the suspension of transactions at the time of trading where criminal activity is suspected—further enhancements to such frameworks should be required from the perspective of user protection. Specifically, as part of their operational control framework, CASPs should establish: (i) a framework for reviewing the crypto-assets they handle; (ii) a framework for providing information on those crypto-assets; (iii) a framework for ensuring that users trade within the limits of their risk tolerance; (iv) a trade monitoring framework; and (v) a framework to ensure that, where an issuer of a crypto-asset violates applicable disclosure requirements, the relevant crypto-asset is discontinued to

[63] For example, this may include operators that provide a broad range of telecommunications-related services.

[64] It has been suggested that operators registered as Type I FIBOs and engaged solely in crypto-asset derivatives may be subject to a prior notification regime similar to that applicable to crypto-asset exchange services.

be handled by the CASP.[65]

With respect to item (iii), given that a large portion of crypto-asset transactions is conducted online, it is necessary to consider specific measures to ensure that the framework operates effectively in terms of client suitability. In addition, further consideration should be given to how the suitability principle[66] under the FIEA can be effectively applied to online financial transactions by individual investors. This should be examined as an issue common to financial transactions generally, including securities transactions.

Furthermore, some CASPs offer services for the purchase and sale of crypto-assets through two types of platforms: "sales platforms" and "trading platforms."[67] Because transactions conducted through "sales platforms" tend to be more profitable for CASPs than those conducted through "trading platforms," concerns have been raised that CASPs may steer customers toward those platforms.[68] Under the FIEA, firms are subject to a best execution obligation, which requires them to establish and implement policies and procedures for executing customer orders on the most favorable terms. From this perspective, consideration should be given to whether the services provided by CASPs to their customers are appropriate.[69]

C. Safeguarding Users' Crypto-assets

With respect to the existing special framework for safeguarding users' crypto-assets—which takes into account the particular risk of unauthorized outflows of crypto-assets—that framework should be

---

[65] It is also important to ensure that CASPs conduct appropriate advertising and promotional activities.

[66] Article 40(1) of the FIEA requires FIBOs to conduct their business in a manner that avoids inappropriate solicitation in light of the customer's knowledge, experience, financial condition, and purpose in entering into the contract.

[67] For the definition of "sales platforms" and "trading platforms," see footnote 45.

[68] Specifically, it has been pointed out that, in the user interfaces of apps provided by CASPs, users can easily access "sales platforms," whereas the route to "trading platforms" may be less apparent.

[69] It has been suggested that, depending on the method of solicitation, such practices could raise issues under the prohibition on false representations (Article 117(1)(ii) of the Cabinet Office Ordinance on Financial Instruments Business, etc.).

maintained under the FIEA.[70] [71] At the same time, in light of the increasingly sophisticated attack vectors seen in recent outflow incidents, additional legal obligations should be introduced. In particular, CASPs should be required to implement enhanced measures for safeguarding users' assets and to strengthen cybersecurity across the entire supply chain. In this regard, it would be appropriate for the detailed content of such measures to be set out not in laws and regulations but in guidelines or similar instruments, so that they can be updated flexibly in response to technological advances and other developments.[72]

In addition, recent incidents have revealed that cyberattacks targeting providers of wallet software used by CASPs may contribute to unauthorized outflows. To prevent the recurrence of such incidents, and while recognizing that CASPs bear primary responsibility for appropriately supervising their contractors, it may be appropriate to introduce regulations applicable to business operators that provide critical systems for the management of crypto-assets to CASPs,[73] in order to ensure the sound operation of such businesses. Specifically, the following regulatory measures should be introduced:

・Such operators should be required to submit prior notifications to the competent authority;

・Such operators should be subject to conduct regulations, including:

(i) disqualification criteria relating to certain past misconduct, such as the revocation of

---

[70] The regulations require service providers to hold crypto-assets of the same type and quantity (performance-guarantee crypto-assets) to provide compensation in the event of outflows of users' crypto-assets managed in hot wallets (i.e., by means other than cold wallets), and to implement the necessary information security measures to prevent information leaks in connection with crypto-asset exchange services.

[71] Regarding the requirement to manage crypto-assets primarily through cold wallets and similar means, it has been suggested that, in light of developments such as emerging technologies relating to signature keys, consideration should be given to whether any revisions are necessary to the regulation of such arrangements under the FIEA.

[72] Where a service provider retains only part of the signature key necessary to transfer a user's crypto-assets, the provider is not regarded as managing those crypto-assets and is therefore not required to register as a CASP. However, if part of the signature key information is lost, users may be unable to transfer their crypto-assets. At present, because individual users primarily use wallets provided by domestic CASPs, there appears to be limited immediate need for regulation. At the same time, given concerns that bringing such services within the scope of crypto-asset exchange services could impose excessive regulatory burdens, it is appropriate to consider, as a future matter, how such services should be regulated.

[73] As the service provider does not manage users' crypto-assets, registration as a CASP is not required under the current law.

registration as a CASP; and

(ii) obligations to ensure the security of systems provided to CASPs; and

- The competent authority should be granted supervisory powers to directly ascertain the state of operations and issue corrective orders.

Furthermore, where a CASP relies on critical systems provided by an external service provider for the management of crypto-assets, it may be appropriate to require that such systems be provided only by operators that have submitted prior notifications.[74]

In designing the details of such regulations, it is important to ensure that the regulatory requirements are set at an appropriate level. Excessive regulatory burdens could lead providers of useful services to withdraw from the market, which could in turn reduce user convenience and undermine system security. It is also important to consider appropriate transitional measures.

D. Liability Reserves

Under current law, CASPs are required, with respect to crypto-assets managed in hot wallets, to secure resources for compensation by holding crypto-assets of the same type and quantity as performance-guarantee crypto-assets. However, crypto-assets managed in cold wallets are also exposed to the risk of outflows due to hacking, and appropriate measures are necessary to ensure that customers can be compensated where necessary. Accordingly, while avoiding the imposition of excessive burdens on CASPs, it may be appropriate to require them to set aside liability reserves at an appropriate level, taking into account factors such as past outflow incidents and applicable cybersecurity standards. In addition, to avoid delays in responding promptly to customers while the causes of outflow incidents are being investigated, it may be appropriate to allow compensation to be paid from liability reserves without prior approval from the competent authority when such incidents occur.

From the perspective of expanding options for securing funds for compensation, consideration should also be given to allowing CASPs to secure such resources through insurance coverage, either as an alternative to or in combination with liability reserves.[75]

---

[74] It has also been suggested that, instead of a prior notification regime, external assurance mechanisms could be used, such as SOC 2 reports (assurance reports on controls relevant to non-financial reporting), contractual restrictions on subcontracting, and obligations requiring subcontractors to cooperate with supervisory authorities' investigations.

[75] Where insurance coverage is permitted as a source of compensation, it is considered a prerequisite that insurance products covering such cybersecurity incidents are adequate and appropriate.

E. Appropriate and Smooth Return of Customer Assets upon Market Exit

When a CASP exits the market, including in the event of bankruptcy, CASPs should also be brought within the scope of the regulations governing customer asset management upon the exit of FIBOs, in order to ensure the appropriate and smooth transfer or return of customer assets, including performance-guarantee crypto-assets.

F. Regulations on Intermediary Business

The 2025 amendments to the PSA established the electronic payment instruments intermediary business and the crypto-asset services intermediary business in order to facilitate services provided by operators that solely intermediate electronic payment instruments and crypto-asset transactions under a proportionate regulatory framework. The basic regulatory framework for the electronic payment instruments intermediary business and the crypto-asset services intermediary business is similar to that for financial instruments intermediary services under the FIEA. For example, both are based on an affiliation framework under which intermediaries for crypto-asset transactions are required to be affiliated with a CASP. Accordingly, if crypto-asset transactions are brought within the scope of the FIEA, the intermediary business relating to such transactions should also be brought within the scope of financial instruments intermediary services under the FIEA. In this context, after necessary transitional measures are established, it may be appropriate, in principle, to apply the regulations applicable to financial instruments intermediary services, including those relating to sales representatives.

G. Borrowing of Crypto-Assets

Operators have developed business models under which they borrow crypto-assets from individual investors and other users, manage them through staking[76] or re-lending, and return them to those users after a certain period together with a borrowing fee. While staking itself is primarily conducted on-chain, operators are increasingly offering staking services[77] to retail users. Under such business models, current regulations governing the management of crypto-assets do not apply to crypto-assets borrowed by the operator (borrower). In addition, users (lenders) are considered to bear various risks, including slashing risks[78] associated with staking and price fluctuation risks associated with the crypto-

[76] A mechanism under which crypto-assets are staked as collateral and rewards are received in crypto-assets in return for participation in activities that support the stable operation of a blockchain.

[77] A service under which a provider stakes crypto-assets on behalf of users and distributes the resulting rewards to them.

[78] A penalty mechanism under which crypto-assets staked may be forfeited as a sanction for misconduct in the course of staking.

assets.

Under current law, borrowing crypto-assets from others does not require registration as a CASP unless it constitutes the "management" of crypto-assets for others.[79] [80] However, from a user's perspective, the business models described above that involve the borrowing of crypto-assets should be subject to the FIEA because, from the users' perspective, they entail assuming risk in pursuit of returns (i.e., borrowing fees). Accordingly, appropriate requirements concerning the establishment of control frameworks and compliance with conduct regulations for borrowed crypto-assets should be imposed as follows. As discussed in Section C above, it is important to ensure that the detailed requirements are set at an appropriate level and that any necessary transitional measures are also considered.

- Obligations to establish risk management frameworks to address counterparty default risk in re-lending and slashing risk arising where the operator (borrower) further entrusts staking to another party;
- Obligations to establish frameworks for the secure management of crypto-assets held in self-custody by the operator; and
- Obligations relating to the provision of risk information to users and compliance with advertising regulations.

It should also be noted that borrowing transactions that are not public in nature—such as those in which institutional investors or retail users borrow crypto-assets from a CASP—should be excluded from the scope of these business regulations.

(3) Treatment of Banks and Insurance Companies and Their Groups

A. Current Treatment

Under the relevant laws and supervisory guidelines, banks and insurance companies, as well as their groups, are currently not permitted to operate crypto-asset exchange services. This reflects the risks associated with crypto-asset-related transactions, including (i) the risk that such transactions may be

---

[79] Where an arrangement is structured as the "borrowing" of crypto-assets but allows the user to demand repayment at any time, thereby resulting in the management of crypto-assets on behalf of others, that arrangement constitutes the management of crypto-assets.

[80] When a CASP borrows crypto-assets, it is required to disclose that such borrowed crypto-assets are not subject to segregated management or preferential repayment, and to establish systems for appropriately managing outstanding liabilities. However, it is not necessary to establish systems specifically for the act of borrowing itself.

misused for money laundering, (ii) system risks involved in the management of crypto-assets, (iii) price volatility risks inherent in holding crypto-assets, and reputational risks if such risks materialize.

Although the acquisition and holding of crypto-assets by banks are not prohibited by law, and banks may in some cases indirectly hold crypto-assets through fund investments, the Ordinance for Enforcement of the Banking Act requires banks to implement measures to ensure appropriate security management and financial soundness in relation to such acquisition and holding. In addition, the supervisory guidelines provide that, where banks hold crypto-assets, such acquisition and holding should be limited to the minimum necessary scope, with holding for investment purposes prohibited, and that adequate risk management and governance frameworks should be in place to avoid impairing core banking operations or causing material losses to the banking group.[81]

B. Treatment by Banks and Insurance Companies Themselves

Allowing banks and insurance companies themselves to issue, purchase, or sell crypto-assets continues to require careful consideration for the following reasons.

- The risks identified in items (i) to (iii) above remain.
- There is a risk that some customers may enter into transactions without adequately assessing the risks of crypto-assets or their own risk tolerance, simply because such products are offered by banks or insurance companies. Accordingly, priority should be given to enhancing user protection by establishing a regulatory framework that treats crypto-assets as financial instruments in a manner that reflects their characteristics. Only thereafter should consideration be given to whether and how such activities should be permitted.

In addition, with respect to crypto-asset intermediation services provided by banks and insurance companies, although the risks borne by those entities may be limited, the second consideration above applies equally. Therefore, careful consideration remains necessary.

Moreover, in light of the current legal framework, under which investment management business by banks and insurance companies themselves is generally prohibited, such entities should also be prohibited from conducting investment management businesses involving crypto-assets.

On the other hand, from the perspective of providing banks and insurance companies with diversification opportunities, it may be appropriate to permit them to hold crypto-assets for their own investment purposes, provided that adequate risk management and governance frameworks are in

[81] Similarly, for insurance groups, the Regulations for Enforcement of the Insurance Business Act and the relevant supervisory guidelines have been put in place.

place.[82]

C. Treatment of Subsidiaries of Banks and Insurance Companies

Subsidiaries of banks and insurance companies may warrant different treatment for the following reasons:

(i) their permissible scope of business is broader than that of banks and insurance companies themselves;

(ii) compared with cases in which such activities are conducted directly by banks and insurance companies themselves, the risk that customers will enter into transactions without adequately assessing the risks of crypto-assets or their own risk tolerance is lower; and

(iii) risks can be appropriately ring-fenced in light of the relationship between subsidiaries and their parent banks and insurance companies.

Accordingly, it would be appropriate to allow such subsidiaries to issue, purchase and sell crypto-assets, and to act as intermediaries in crypto-asset transactions, thereby ensuring a level playing field between FIBO within bank and insurance groups and other such operators. Similarly, it would be appropriate to allow such subsidiaries to conduct investment management businesses involving crypto-assets and to hold crypto-assets for their own investment purposes. The same treatment should also apply to sister companies and affiliates of banks and insurance companies.

(4) Measures Against Unregistered Operators

A. Measures Against Unregistered Operators

To deter illegal solicitation by unregistered operators, penalties should be strengthened by bringing the purchase and sale of crypto-assets within the scope of the financial instruments business under the

[82] It has been suggested that discussions on whether banks and insurance companies should be permitted to hold crypto-assets for investment purposes—and, if so, what risk management frameworks should be required—could also affect consideration of whether other public-interest institutional investors should be permitted to invest in crypto-assets. Accordingly, such matters should be considered in light of these potential impacts.

FIEA.[83] [84]

In addition, the provisions of the FIEA relating to measures against unregistered operators should also apply to crypto-asset exchange services. These should include: prohibiting unregistered operators from representing that they intend to conduct such services; authorizing courts to issue emergency injunctions; and authorizing the SESC to file petitions for such injunctions, together with granting the necessary powers to conduct criminal investigations for that purpose.

While careful consideration is required as to whether purchase and sale agreements with unregistered operators should be uniformly presumed to constitute unconscionable transactions, given that there are cases in which domestic residents conduct transactions with foreign unregistered operators, it may nevertheless be appropriate, in light of user harm caused by fraudulent solicitations by unregistered operators, to establish civil law provisions to address such conduct, including provisions under which such contracts may be deemed void.[85]

B. Measures Against Inappropriate Conduct in Investment Management

In light of the increasing prevalence of crypto-asset investment seminars and online communities, investment management and investment advisory services related to crypto-assets should be brought within the scope of the regulatory frameworks applicable to investment management business and investment advisory business, in order to ensure their proper operation.[86]

C. Preventive Measures Against User Harm Through Payment Means

To proactively prevent crypto-assets from being used as a means of payment in fraudulent investment solicitations, CASPs should be required, by laws and regulations, to implement measures such as:

---

[83] Under current law, providing crypto-asset exchange services without registration is punishable by imprisonment for up to three years, a fine of up to three million yen, or both. By contrast, under the FIEA, conducting financial instruments business without registration is punishable by imprisonment for up to five years, a fine of up to five million yen, or both.

[84] It has been suggested that the maximum term of imprisonment for conducting financial instruments business without registration be increased to 10 years.

[85] With respect to shares, in light of investor losses arising from transactions in unlisted shares conducted by unregistered operators, provisions have been established under which purchase and sale agreements for unlisted shares entered into by unregistered operators are presumed to constitute exploitative practices and are, in principle, deemed void (Article 171-2 of the FIEA).

[86] It has been suggested that investment management service providers dealing in crypto-assets be required to establish appropriate cybersecurity frameworks, depending on the nature of their transactions.

(i) issuing warnings about the risk of fraudulent activity and confirming the purpose of the transfer when users transfer crypto-assets to unhosted wallets or wallets operated by unregistered operators;

(ii) conducting appropriate transaction monitoring; and

(iii) establishing a cooling-off period or other deliberation period immediately after account opening and before transfers to newly designated wallets.

In addition, some CASPs have already implemented such measures, and SROs are expected to disseminate good practices adopted by CASPs so that these initiatives can be promoted across the industry as a whole.

(5) Measures Against Foreign Unregistered Operators and DEXs

A. Measures Against Foreign Unregistered Operators

Currently, where foreign unregistered operators solicit domestic residents through Japanese-language websites, the authorities take measures such as issuing warnings, making public announcements, and requesting app stores to remove the relevant applications. Going forward, efforts should continue to focus on these measures, while measures against unregistered operators should be further strengthened and investigative cooperation with foreign authorities enhanced.

Under the FIEA, foreign securities firms are permitted, without solicitation, to accept orders from domestic residents and execute transactions.[87] It may be appropriate to establish a similar regulatory framework for crypto-asset transactions and to clarify the scope of the relevant regulations.[88]

B. Measures Against DEXs

Although there is no clear definition of decentralized exchanges (DEXs), they are currently generally understood to exhibit the following characteristics:

---

[87] In principle, advertisements posted by foreign securities companies on websites regarding activities relating to securities-related businesses shall be deemed to constitute solicitation. However, such advertisements shall not be deemed to constitute solicitation targeting investors in Japan, provided that reasonable measures are taken to prevent them from leading to securities-related business activities with investors in Japan as counterparties. (Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc., X-1-2).

[88] However, in such cases, it may be unclear which regulations apply to foreign exchange service providers, protections available under Japanese law may not apply, and dispute resolution may be difficult. This may put users at a disadvantage. Accordingly, it is important to enhance user literacy through the provision of information by the authorities and other relevant parties.

・Unlike centralized trading platforms, in which an operator manages or intermediates transactions, users can exchange crypto-assets autonomously through direct peer-to-peer (P2P) communications using smart contracts;

・Operating policies are determined through voting by governance token holders, and there is no centralized controlling entity, or such an entity is difficult to identify;

It has also been noted that some services describing themselves as DEXs are, in fact, centralized in nature.

In their current form, DEXs enable users to exchange crypto-assets through protocols developed and deployed by developers. Under the current legal framework, such activities may, in certain cases, fall within the scope of crypto-asset exchange services. At the same time, it should be noted that such protocols are characterized by the absence of direct solicitation by developers and by the limited human intervention involved once they have been deployed. In addition, certain DEXs are considered to fall outside the regulatory perimeter in Europe and the United States. At the same time, DEXs involve risks, including losses to users resulting from protocol vulnerabilities and the risk that they may be misused for money laundering.

In light of these considerations, although no clear regulatory approach to DEXs has yet been established, it is appropriate to continue examining proportionate regulatory frameworks tailored to their technical characteristics and distinct from those currently applied to CASPs, while closely monitoring regulatory and supervisory developments in other jurisdictions.

Furthermore, with regard to entities that provide user interfaces (UIs), such as applications that connect users in Japan to DEXs, it is first necessary to deepen understanding of the actual nature of such services, while monitoring regulatory developments in other jurisdictions, with a view to introducing proportionate and risk-based regulation. Such regulation may include obligations to explain the risks associated with the relevant DEX, as well as AML/CFT requirements, including customer due diligence obligations under the APTCP.

In addition, given that AML/CFT measures for transactions conducted through DEX protocols or related UIs may extend beyond a single jurisdiction, it is appropriate to continue international discussions on this matter.

As an immediate measure, government authorities and CASPs should adequately inform users that transactions through DEXs or unregistered operators in Japan may expose them to unexpected losses.[89]

---

[89] It has been suggested that, in addition to DEXs, it is also necessary to understand the actual state of DeFi (decentralized finance) when considering future regulatory approaches.

5. Enhancing Literacy Related to Crypto-Asset Transactions

(1) Measures to Promote Prudent Trading by Users

To ensure that users fully understand the risks and product characteristics and trade within their risk tolerance, CASPs should be prohibited from making representations that impede proper risk recognition or encourage speculative trading, for example, by placing undue emphasis on past performance or future projections. CASPs should also be required to establish frameworks to ensure that customers trade within their risk tolerance. In addition, CASPs should ensure the proper implementation of measures, in accordance with self-regulatory rules, such as establishing criteria for the commencement of transactions and setting limits on transaction amounts and holdings.

(2) Raising Awareness of the Risks of Transactions on DEXs or with Unregistered Foreign Operators

Administrative authorities and CASPs should inform users that transactions on DEXs or with unregistered foreign operators may expose them to the risk of unforeseen losses. Administrative authorities and CASPs should ensure that such risks are communicated clearly and widely.

(3) Measures to Enhance Financial Literacy Related to Crypto-Asset Transactions

To ensure user protection, CASPs should provide adequate explanations and conduct customer suitability assessments. These measures are intended to ensure that users sufficiently understand the risks and engage in transactions within their financial capacity. In addition, it is appropriate to adopt a multifaceted approach to raising user awareness. This should include awareness-raising initiatives by administrative authorities, CASPs, and the Japan Financial Literacy and Education Corporation (hereinafter, "J-FLEC").

J-FLEC's educational materials already include warnings about solicitations involving complex products, including crypto-assets. Going forward, through revisions to such materials and other initiatives, efforts should be made not only to prevent financial harm arising from fraudulent solicitations involving crypto-assets, but also to enhance users' understanding of the key risks and characteristics of crypto-assets, including:

・Crypto-assets are subject to significant price volatility.

・Compared with traditional financial instruments such as stocks and bonds, crypto-assets have a relatively short trading history; accordingly, established valuation methods have not yet been developed.

・There is a risk of irreversible loss if users make errors, such as transferring crypto-assets to the wrong address.

・Crypto-assets managed by CASPs may be exposed to the risk of hacking or other security incidents, and if such risks materialize, users' crypto-assets may be adversely affected.

・ Users should engage in crypto-asset transactions only after sufficiently understanding the associated risks and product characteristics, and only to the extent of their surplus funds.

6. Cybersecurity Initiatives

(1) Basic Principles of Cybersecurity Initiatives

With respect to cybersecurity measures relating to crypto-assets, laws and regulations should stipulate obligations to establish the necessary organizational frameworks. Technical and operational requirements, however, should be set out in guidelines to allow flexible responses to changes in the operating environment, given that threat actors are becoming increasingly sophisticated and CASPs' system architectures are constantly evolving through technological innovation. The protection of users' crypto-asset-related assets should be premised on robust cybersecurity. Accordingly, it is important that each company's risk management PDCA cycle functions effectively, supported by adequate investment in cybersecurity. In designing requirements under laws, regulations and guidelines, due consideration should be given to incentives for, and feasibility of, such investments by CASPs.

(2) Industry Collaboration and the FSA's Initiatives

To date, the FSA has promoted the government-led cybersecurity initiatives for the financial industry, including CASPs, by issuing guidance (including the "Guidelines on Cybersecurity for the Financial Sector"), conducting monitoring, and implementing exercises such as Delta Wall. It is important to continue these initiatives steadily.

Furthermore, numerous cyber incidents resulting in outflows of crypto-assets have occurred worldwide, and in recent cases, attack techniques have become increasingly sophisticated. Accordingly, public–private efforts to continuously strengthen cybersecurity frameworks at CASPs and related entities have become essential. As individual firms are continuously exposed to sophisticated attacks, including those by nation-state-level actors, cybersecurity management should be strengthened through a combination of self-help, mutual assistance, and government support. In particular, as the development of industry-wide mutual assistance initiatives is essential, [90] information-sharing bodies, including JP Crypto-ISAC, are expected to function effectively. The FSA should actively support these efforts.

7. Regulations on Market Establishment

The FIEA provides for a market establishment regime for securities and derivatives. With respect to crypto-asset derivative transactions (margin trading), which fall within the scope of the FIEA, some operators offer order-book trading by matching users' orders. However, such trading venues are not currently considered to constitute a financial instruments market and are therefore not subject to the licensing requirements applicable to financial instruments exchanges.

By contrast, the PSA does not provide for a market-establishment regime for spot crypto-asset transactions. Nevertheless, some CASPs operate so-called exchanges that match customers' orders through order-book trading. In this context, a key issue is whether such crypto-asset exchanges should be made subject to a market-establishment regime.

Crypto-asset exchanges provide trading venues where transactions are conducted among a large number of participants. Accordingly, appropriate trading controls and system arrangements are necessary to ensure fair and neutral price formation and business operations. At the same time, given the nature of crypto-assets, the price-discovery function of individual crypto-asset exchanges remains limited. For this reason, there appears to be limited need for stringent market-establishment regulations,[91] such as the licensing regime applicable to Financial Instruments Exchanges or the regulatory framework for proprietary trading systems (PTSs).

A separate issue is whether existing Financial Instruments Exchanges should be permitted to handle spot crypto-assets. If a Financial Instruments Exchange were to provide a venue for crypto-asset transactions in a manner similar to that of a CASP, it would likely need to hold customers' crypto-assets off-chain and transfer them between the accounts of transaction counterparties. In that case, the Exchange would bear the risk of customer asset outflows resulting from hacking or other security

---

[90] It has been suggested that collaboration with other sectors is also an important issue that the crypto-asset industry should address.

[91] For example, it may be appropriate to require appropriate trading controls and system arrangements to ensure fairness and neutrality in price formation and business operations, with reference to regulatory frameworks such as the registered PTS regime, which is less restrictive than the authorized PTS regime.

incidents. Depending on the scale of the market, such risks could become substantial and, in turn, materially affect the Exchange's operation of securities or derivatives markets. Accordingly, caution is warranted at this stage in considering whether to permit the handling of spot crypto-assets on Financial Instruments Exchanges.

8. Market Abuse Regulations

With respect to market abuse regulations for crypto-assets, the 2019 amendments to the FIEA introduced a general prohibition on wrongful acts, as well as provisions prohibiting the spreading of rumors, the use of fraudulent means, and market manipulation, similar to those applicable to listed securities. However, given the difficulty of defining in advance both "insiders" and "non-public material facts that would significantly affect customers' investment decisions," the FIEA does not currently contain provisions that directly regulate insider trading in crypto-assets.[92] In addition, although criminal penalties are available for market abuse, neither an administrative monetary penalty system nor SESC authority to investigate criminal violations has been established. In light of this, there are concerns that the deterrent effect is insufficient.

(1) Insider Trading Regulations

In recent years, IOSCO has issued recommendations aimed at preventing market abuse.[93] In addition, jurisdictions such as the EU and the Republic of Korea have introduced insider trading regulations for crypto-assets,[94] and enforcement actions relating to insider trading involving crypto-assets have also been brought in the United States.[95] In Japan, as crypto-assets increasingly come to be regarded as investment assets, the need to deter market abuse that could undermine the fairness of

---

[92] FSA, "Report from Study Group on Virtual Currency Exchange Services". (December 21, 2018)

[93] See footnote 19.

[94] In Europe, MiCA became fully applicable at the end of December 2024. In the Republic of Korea, the Act on the Protection of Virtual Asset Users came into force in July 2024.

[95] Between June 2021 and April 2022, an employee of Coinbase, the largest crypto-asset trading platform in the United States at the time, provided relatives and others with non-public information regarding the timing and content of announcements of newly handled crypto-assets. The recipients of the information are alleged to have earned at least USD 1.1 million by trading on the basis of that information.

In July of that year, the U.S. Department of Justice filed criminal charges, and the SEC brought a civil enforcement action. In the criminal case, the relative was sentenced to 10 months' imprisonment in January 2023, and the employee was sentenced to two years' imprisonment in May 2024. In the civil action, the SEC prevailed in March 2024.

crypto-asset trading and to ensure a sound and fair trading environment has become more pronounced. In light of these international and domestic developments, insider trading regulations for crypto-assets should be established.[96]

A. Protected Legal Interest

Under the insider trading regulations applicable to listed securities, the protected legal interest is the preservation of investor confidence in the fairness and integrity of the securities markets. In developing insider trading regulations for crypto-assets, it is appropriate to define the protected legal interest as the protection of users' confidence in the fairness and integrity of trading venues provided by domestic CASPs, for the following reasons:

・Regulated Trading Venues:

Domestic CASPs are subject to conduct regulations under Japanese law, and the crypto-assets they handle are subject to review by self-regulatory organizations (SROs). For this reason, users are likely to have greater confidence in the fairness and integrity of trading venues provided by domestic CASPs than in trading through foreign operators or decentralized exchanges (DEXs).

・Trading Practices of Retail Investors:

Retail investors primarily trade through accounts opened with domestic CASPs. Accordingly, there is a greater need to protect their confidence in the trading venues provided by such CASPs.

B. Principles for Regulation

To protect the legal interest described above, it is necessary to prohibit insiders from engaging in transactions that would undermine users' confidence in trading venues. Specifically, with respect to (i) "covered crypto-assets," (ii) persons who have access to material facts (iii) by virtue of a special position are prohibited from engaging in (iv) transactions before publication of such material facts that would (v) undermine users' confidence in trading venues. From the perspective of regulatory clarity, it would be appropriate to use the framework for insider trading regulations applicable to listed securities as the basis, while making the necessary adjustments to reflect the characteristics of crypto-assets.

(i) Covered Crypto-Assets

To protect the legal interest described above, the scope of crypto-assets subject to insider trading regulations should be limited to those handled by domestic CASPs. As with the insider trading regulations for listed securities, the regulations should apply irrespective of the trading venue so as to

---

[96] For an overview of insider trading regulations applicable to crypto-assets, see Section V, Reference Material 4.

cover transactions on DEXs and direct peer-to-peer transactions.

In addition, crypto-assets for which a formal application for handling has been submitted to a CASP should also be included in the scope of the regulation. Even before a crypto-asset is handled by a domestic CASP, there is a risk of insider trading exploiting price movements associated with its prospective handling by a CASP, as evidenced by enforcement cases in other jurisdictions. To ensure clarity regarding the scope of the regulation, SROs should provide a comprehensive list of crypto-assets handled by domestic CASPs in a clear and accessible manner. The same approach should apply to crypto-assets for which formal applications for handling have been submitted to CASPs.

(ii) Material Facts

Although there has not yet been sufficient practical experience regarding what constitutes material facts for crypto-assets, it is important to ensure predictability and transparency in the regulatory framework. Accordingly, with reference to the insider trading regulations applicable to listed securities,[97] it may be appropriate to enumerate events that clearly constitute "material facts," supplemented by a basket clause. Specifically, events falling within the following three categories that may affect users' trading decisions should be individually specified as "material facts", and a basket clause should be introduced to cover other cases that do not fall within these categories:[98]

- Material facts relating to the business or affairs of issuers of crypto-assets with an identifiable issuer (e.g., the bankruptcy of the issuer or the discovery of significant security vulnerabilities[99]).
- Material facts relating to the handling of crypto-assets by CASPs (e.g., the commencement or discontinuation of such handling, or incidents involving the outflow of crypto-assets).
- Material facts relating to large-volume transactions (e.g., the purchase or sale of 20% or more of

[97] Under insider trading regulations for listed securities, material facts are categorized as internal information and external information relating to the issuer. Internal information consists of facts that arise within the issuer and decided by the issuer and are likely to affect investors' decisions; such facts are enumerated as specifically as possible and supplemented by a basket clause.
[98] It has been suggested that adopting regulations analogous to the existing insider trading regulations for listed securities may fail to capture external information, a key factor in crypto-asset price formation, and that a more flexible approach may therefore be appropriate.
[99] In addition, for crypto-assets with an identifiable issuer, where they are used as a means of payment for specific services, the discontinuation of such services may be considered an event relating to the issuer's business activities.

the issued crypto-assets[100]).

(iii) Insiders

As with the insider trading regulations applicable to listed securities,[101] persons who are in a special position to access material facts and who become aware of such information by virtue of that position should be subject to these regulations. Specifically, depending on the category of material facts, the following persons should be covered. As under the insider trading regulations for listed securities, such persons should include officers, persons exercising authority under laws or regulations, and contractual counterparties. First-level recipients of information from such persons should also be covered.

- For material facts relating to the business or affairs of issuers of crypto-assets with an identifiable issuer: persons related to such issuers
- For material facts relating to the handling of crypto-assets by CASPs: persons related to such CASPs
- For material facts relating to large-volume transactions: persons related to such transactions

Crypto-assets may be handled by CASPs without the involvement of the issuer of the relevant crypto-asset, for example, where a CASP independently commences handling such a crypto-asset. Accordingly, persons related to CASPs are included among the parties subject to regulation with respect to material facts relating to the handling of crypto-assets by CASPs.[102]

(iv) Public Disclosure Measures

As in the case of insider trading regulations for listed securities,[103] it may be appropriate, depending

---

[100] Cases in which the equity method is applied under applicable accounting standards may serve as a useful reference.

[101] Insider trading regulations for listed securities apply to persons in a special position—such as those associated with a listed company or a tender offeror—who become aware of internal information by virtue of that position.

[102] In overseeing and providing them with guidance for the sound development of the crypto-asset exchange industry, the self-regulatory organization (JVCEA) is regarded as a “person having authority under law” in relation to CASPs and is therefore subject to regulation.

Similarly, in the context of insider trading regulations for listed securities, financial instruments exchanges and SROs that perform self-regulatory functions relating to listings under the FIEA are regarded as “persons having authority under law” in relation to issuers.

[103] Under insider trading regulations for listed securities, in order to determine clearly whether a transaction is subject to sanctions, the methods of disclosure are limited, depending on the type of

on the category of material facts, to designate the following persons as the entities responsible for public disclosure.

- For material facts relating to the business or affairs of issuers of crypto-assets with an identifiable issuer: the relevant issuer
- For material facts regarding the handling of crypto-assets by CASPs: the relevant CASPs
- For material facts relating to large-volume transactions: the person conducting the relevant transactions

With respect to the means of public disclosure, social media platforms present a number of challenges. These include the wide variety of platforms, the limited dissemination of information among users, the ease with which posted content can be deleted or altered, and the lack of assurance as to the authenticity of the source and the content of such information. For this reason, the means of public disclosure subject to regulation should, at present, be limited to publication on the websites of CASPs and SROs. In particular, SROs should establish frameworks for the prompt disclosure of material facts notified by the relevant disclosure entities.

(v) Prohibited Acts and Exemptions

As with the insider trading regulations for listed securities,[104] purchases and sales should, in principle, constitute prohibited acts. In addition, from the perspective of user protection at the time of initial issuance, it may be appropriate to include the initial issuance of crypto-assets and corresponding primary acquisitions within the scope of prohibited acts. Such acquisitions should be limited to acquisitions for consideration and should exclude acquisitions through mining and similar activities.

With respect to exemptions, there is currently only limited experience regarding the categories of transactions that need not be regulated in light of the legally protected interest applicable to crypto-assets. Accordingly, it may not be sufficient to apply to crypto-assets the exemptions currently provided under the insider trading regulations for listed securities. At the same time, given that evidence relating

---

material fact, to certain legally prescribed means of public announcement by specified entities. These include: (i) public inspection of securities registration statements and similar documents; and (ii) measures to make information publicly available, such as (a) the lapse of 12 hours after the information has been disclosed to two or more news media organizations, or (b) notification to a financial instruments exchange and the making the information publicly available on the exchange's website.

[104] Under insider trading regulations for listed securities, "purchase and sale" are defined as prohibited acts and include transactions that transfer ownership, such as sales, exchanges, and contributions in kind. However, because investor protection at the issuance stage is ensured under the Companies Act, initial acquisition upon issuance is not treated as a prohibited act.

to a transaction is often concentrated in the hands of the person engaging in that transaction, it may be appropriate to introduce an exemption where that person can demonstrate that the transaction would have been executed even without knowledge of the material facts. This would help ensure that only conduct warranting regulation in light of the protected legal interest is captured.

C. Prohibition of the Communication of Non-Public Material Facts and Trading Recommendations

As with the insider trading regulations for listed securities,[105] users' confidence in the fairness and soundness of trading venues provided by domestic CASPs cannot be fully maintained unless the communication of non-public material facts and trading recommendations in relation to crypto-assets is prohibited. Accordingly, together with the introduction of insider trading regulations, it may be appropriate to prohibit the communication of non-public material facts and trading recommendations where they are made for the purpose of enabling another person to gain profits or for other similar purposes.

(2) Other Market Abuse Regulations

For securities, market abuse regulations include not only the general prohibition of wrongful acts and prohibitions on the spreading of rumors, the use of fraudulent means, market manipulation, and insider trading, but also other measures, such as the prohibition of stabilization transactions. As measures to address market abuse involving crypto-assets are strengthened, market abuse regulations applicable to crypto-assets should be introduced, as appropriate. For example, the prohibition of stabilization transactions[106] should be extended to crypto-assets, as the rationale underlying that prohibition applies equally to such assets. In addition, to address so-called stealth marketing, disclosure requirements applicable to persons who receive consideration for expressing opinions relevant to trading decisions on websites or other online platforms should also be extended to crypto-assets.

Under the insider trading framework described above, insider trading regulations would not apply to crypto-assets handled exclusively by unregistered operators. Nor would they generally apply where

---

[105] With respect to listed securities, the communication of non-public material facts or recommendations to trade for the purpose of conferring a benefit is prohibited because such conduct promotes insider trading, increases the likelihood of such trading, enables favorable transactions by persons in positions close to insiders, and may undermine the protected legal interest in ensuring investor confidence in the fairness and soundness of the market.

[106] This regulation is intended to prevent market participants who mistakenly believe that a price maintained through stabilization activities reflects natural supply and demand from suffering losses when prices move after the termination of stabilization transactions (Article 159(3) of the FIEA).

a person trades while in possession of material non-public external information relating to a crypto-asset handled by a domestic CASP, except in relation to certain categories of information, such as large-volume transactions. In addition, forms of market abuse unique to crypto-assets that cannot be adequately addressed under existing FIEA provisions may emerge. Some of these activities may nevertheless be addressed under existing provisions, including the general prohibition of wrongful acts and the prohibition of the use of fraudulent means. However, crypto-assets are traded globally and often exhibit a high degree of anonymity, and there are therefore practical limits to preventing all forms of misconduct involving crypto-assets in a timely manner. Going forward, market abuse involving crypto-assets should continue to be closely monitored. If, in light of actual enforcement cases and observed market practices, it becomes apparent that additional measures are needed to address recurring forms of misconduct, further regulatory responses should be considered.

(3) Administrative Monetary Penalties Framework and Other Enforcement Measures

To ensure the effectiveness of market abuse regulations, it is important to maintain robust enforcement mechanisms and strengthen deterrence against violations.

A. Administrative Monetary Penalty Framework

Under the FIEA, the administrative monetary penalty framework serves as an administrative measure to impose monetary sanctions that effectively deter violations in financial and capital markets and ensure the effectiveness of regulatory requirements. An administrative monetary penalty framework should also be established for crypto-assets to address market abuse, including insider trading, in a manner comparable to the framework applicable to listed securities.

B. Criminal Investigative Authority and Investigative Authority for Administrative Monetary Penalties

To ensure the effectiveness of market abuse regulations, the SESC should be granted the authority to conduct criminal investigations into market abuse involving crypto-assets, as in cases involving listed securities. The SESC should also be granted the investigative authority necessary to administer the administrative monetary penalty framework. In addition, the SESC's organizational capacity should be strengthened accordingly.

C. Market Surveillance Framework

With respect to market abuse involving listed securities, FIBOs are required to establish trade monitoring systems designed to prevent such abuse. In addition, within the Japan Exchange Group, Japan Exchange Regulation conducts trade surveillance and reports detected cases of market abuse to the SESC. Together, these measures have contributed to the establishment of an effective market surveillance framework. For crypto-asset trading, trade monitoring by CASPs and market surveillance by SROs should likewise be significantly strengthened to ensure effective enforcement.[107]

D. Investigative Cooperation with Foreign Regulatory Authorities

Crypto-assets can be traded across borders with ease. In addition, it is necessary to address cases in which foreign investors engage in market abuse on trading venues operated by domestic CASPs. For these reasons, cooperation with foreign regulatory authorities is essential to ensure the effectiveness of market abuse regulations. Accordingly, crypto-asset transactions should also be brought within the scope of investigative cooperation arrangements with foreign regulatory authorities, on a reciprocal basis, as is the case with securities transactions.[108]

[107] Specifically, possible measures include enhancing trade monitoring capabilities at the level of each CASP, such as by developing detection criteria for different types of market abuse and strengthening measures based on the results of such monitoring, establishing a market surveillance framework at the SRO level, including the collection of trading data from members and the detection and review of market abuse, and strengthening information-sharing among CASPs, the SRO, and the authorities.

[108] Under the FIEA, if a foreign financial regulatory authority requests cooperation in connection with an administrative investigation conducted to enforce a foreign law equivalent to the FIEA, and if it is deemed appropriate to provide such cooperation, the FSA may require reports and take other necessary measures, to the extent necessary and appropriate to respond to the request (Article 189 of the FIEA).

IV. Conclusion

This Report summarizes the matters deliberated by this Working Group since July 2025. Going forward, relevant stakeholders are expected to take the necessary actions in light of this Report, thereby further enhancing user protection and improving the trading environment.

Japan has been at the forefront of developing regulatory frameworks for crypto-assets. This regulatory review is expected to further enhance the soundness of Japan's crypto-asset market and strengthen its international credibility.

At the same time, this regulatory review focuses primarily on transactions conducted through domestic CASPs, where the need for user protection and a sound trading environment is particularly significant. It should therefore be recognized that this review covers only a portion of global crypto-asset trading. Nor will this review, by itself, ensure the soundness of the entire crypto-asset market. Crypto-asset transactions conducted outside CASPs constitute highly anonymous segments of the market, including transactions on DEXs, where effective regulation cannot at present be sufficiently imposed on a global basis. Going forward, continued cooperation among regulatory authorities across jurisdictions will be essential to developing appropriate responses. In addition, the impact of this regulatory review should be appropriately monitored through ongoing assessment of developments in the crypto-asset market and related businesses. Where technological developments or market practices reveal regulatory gaps or unnecessary burdens, the regulatory framework should be kept under review and refined as necessary.

V. Reference Materials

This chapter presents, for reference, materials used by the Working Group to help readers understand the overall framework of this regulatory review. It should be noted that certain descriptions have been revised from the versions originally used at each meeting in light of subsequent discussions by the Working Group.

Material 1: Overall Framework for Disclosure Requirements

(Source: Prepared based on page 2 of Material 2 for the 5th Meeting (Nov. 7) of this Working Group)

Overall Framework for Disclosure Requirements (1)

	Crypto-assets with an identifiable issuer	Other crypto-assets
	The issuer raises funds through the offering	The issuer does NOT raise funds through the offering
Disclosure items (upon commencement of handling)	・ The characteristics and functionality of the crypto-assets, total number of the crypto-assets, underlying technology, rights and obligations attached to the crypto-assets, and associated risks	
	・ Information about the issuer, planned use of the offering proceeds, the crypto-asset project	—
Entities subject to the regulation	***Issuer*** obliged to prepare and disclose information ***CASPs*** *(crypto-asset exchange service providers)* obliged to disclose information prepared by the issuer	***CASPs*** obliged to prepare and disclose information
Acts subject to the regulation	Fundraising through the sale of crypto-assets by the issuer*	Handling of crypto-assets by CASPs
Exemptions	In cases equivalent to private placements or private secondary distribution (i.e., solicitation to a small number of investors or to qualified institutional investors)	
Method and Timing	・Publication on the websites of the issuer or CASPs ・Prior to solicitation by CASPs	・ Publication on the websites of CASPs ・ Prior to solicitation by CASPs

**Offers provided free of charge, and distributions created automatically as a rewards for mining or staking, are exempt from this regulation.*

Overall Framework for Disclosure Requirements (2)

		Crypto-assets with an identifiable issuer	Other crypto-assets
		The issuer raises funds through the offering	The issuer does NOT raise funds through the offering
Ongoing Disclosure	Frequency	・ Timely disclosure (prescribed by law) ・ Periodic (annual) disclosure (prescribed by law)	・ Timely disclosure (prescribed by law) ・ Periodic disclosure (under self-regulatory rules)
	End of Disclosure	In the following cases, disclosure requirements are exempted or waived. ***Issuer*** ・ Terminated if the crypto-asset is decentralized ・ Exempted if all domestic CASPs discontinue handling the crypto-asset ***CASPs*** ・ Exempted if the CASPs discontinue handling the crypto-asset	***CASPs*** Exempted if the CASPs discontinue handling the crypto-asset
Ensuring Accuracy and Objectivity		・ Criminal penalty, civil liability, and administrative monetary penalty for material misstatements and omissions ・ Suspension of handling by all domestic CASPs if the issuer violates disclosure requirements ・ Enhancement of the gatekeeping function of CASPs and a self-regulatory organizations (SRO)	
User Protection		・ Setting an investment limit for users, similar to equity crowdfunding ・ Preventing conflicts of interest between the issuer and CASPs, and explaining conflicts of interest to investors ・ Prohibiting preferential issuance to specific persons before or after “listing,” and imposing lock-up periods for insiders (prohibiting sales for a certain period)	—

Material 2: Application of Disclosure Requirements and Regulations on Crypto-related Business
(Source: Prepared based on page 31 of Material 4 for the 4th Meeting (Oct. 22) of this Working Group)

Application of Disclosure Requirements and Regulations on Crypto-related Business

Type of Conduct	Scope of Crypto-Assets	Subject Entities	Disclosure requirements	Regulations on Crypto-related Business	
Sale of newly issued and outstanding crypto-assets by the issuer	Crypto-assets with an identifiable issuer	**Issuer**	Obligation to prepare and disclose information*	Sales through CASPs	Registration Not Required
				Sales by the issuer itself	Registration Required*
		CASPs	Obligation to disclose information (that the issuer prepared)*	Intermediation of sales	Registration Required
Purchasing and selling crypto-assets (excluding cases above)	Crypto-assets (regardless of whether an identifiable issuer exists)	**CASPs**	Obligation to prepare and disclose information	Purchase and sale, or intermediation (as a business)	Registration Required

**The following cases are exempted from this requirement:*
(i) offers to 49 or fewer persons (excluding Qualified Institutional Investors), subject to transfer restrictions
(ii) offers exclusively to Qualified Institutional Investors, subject to transfer restrictions.

Material 3: Basic principles of Regulations on Crypto-related Business

(Source: Prepared based on page 4,5 of Material 4 for the 4th Meeting (Oct. 22) of this Working Group)

Basic principles of Regulations on Crypto-related Business (1)

- Where an entity conducts the business of purchasing and selling crypto-assets, the entity should, in principle, be subject to regulations equivalent to those applicable to Type I financial instruments business. In addition, with respect to provisions under the current PSA that reflect the specific nature of crypto-assets, corresponding provisions should be introduced into the FIEA, as there are currently no equivalent provisions applicable to Type I financial instruments business.

Major regulations	Crypto-asset exchange services	Type I financial instrument business
Major shareholder regulations	-	✓
Financial soundness requirements (capital and net assets)	✓（more than 10 million yen）	✓（more than 50 million yen）
Requirement to be a stock company	✓	✓
Mandatory establishment of a board of directors	-	✓
Exemptions from special provisions for privately held companies under the Companies Act	-	✓
Notification requirements for the appointment of directors and officers	-	✓
Regulation of non-core business activities	-	✓
Establishment of operational control frameworks	✓	✓
Capital adequacy ratio	-	✓
Obligation to set aside liability reserves	-	✓
Requirement to display statutory signage and to make trade name information available for public inspection	-	✓
Prohibition of name lending	✓	✓
Regulations on advertising	✓	✓
Obligation to indicate transaction terms in advance	✓	✓
Obligation of disclosure and explanation prior to contract conclusion	✓	✓
Obligation of disclosure at the time of contract conclusion	✓	✓
Obligation to provide documents upon receipt of security deposits	✓	✓
Obligation to conclude a contract with a designated dispute resolution organization	✓	✓
Obligation to segregate users' assets	✓	✓
Performance-guarantee crypto-assets	✓	-
Right to receive priority payment of crypto-assets	✓	-

Basic principles of Regulations on Crypto-related Business (2)

Major regulations	Crypto-asset exchange services	Type Ⅰ financial instrument business
Obligation to prepare short-term reports when managing customer assets	✓	-
Prohibition of misrepresentation and false announcement	✓	✓
Prohibition of providing conclusive assessment, prohibition of providing uninvited solicitation, obligation to confirm customers' intention to receive solicitation, and prohibition of repeated solicitation	✓	✓
Prohibition of solicitation at inappropriate times	-	✓
Prohibition of abuse of officers' positions, prohibition of accepting orders for insider trading, and prohibition of solicitation based on corporate-related information	-	✓
Prohibition of front running and market manipulative trading	✓	✓
Prohibition of simultaneous or excessive solicitation for specific limited crypto-assets and large-volume recommendation sales	-	✓
Prohibition of proprietary trading against customers in margin transactions	-	✓
Regulations related to short selling	-	✓
Prohibition of loss compensation	-	✓
Principle of suitability	✓	✓
Obligation to establish and disclose best execution policy	✓	✓
Restriction on the act of furnishing a customer's securities or crypto-assets as collateral	-	✓
Prohibition of accepting orders subject to granting credit	-	✓
Restriction on granting credit by underwriters	-	✓
Flexible application of regulations for transactions with professional investors	-	✓
Public inspection of explanatory documents	-	✓
Obligation to file a post-event notification when a single entity comes to hold a majority of the voting rights	-	✓
Registration system for sales representatives	-	✓
Information security management	✓	✓
Prior notification requirements upon commencement of handling of crypto-assets	✓	-
Supervision of outsourced contractors	✓	△(Guidelines)
Customer due diligence obligations at the time of transaction under the APTCP	✓	✓
Travel Rule under the APTCP*	✓	-

** When a CASP transfers crypto-assets to a wallet managed by another CASP upon the user's request, it must transmit information on the originator and beneficiary (Article 10-5 of the APTCP). This requirement is referred to as "Travel Rule."*

Material 4: Overall Framework of Insider Trading Regulations involving Crypto-assets

(Source: Prepared based on page 37 of Material 2 for the 5th Meeting (Nov. 7) of this Working Group)

Overall Framework of Insider Trading Regulations involving Crypto-assets

Overall	With respect to (1) 'covered crypto-assets', it is prohibited for persons who can gain access to (2) 'material facts' by virtue of a special position ((3) insiders), prior to (4) 'publication' of such facts, to conduct (5) transactions that would undermine users' confidence in trading venues.		
(1) Scope (covered crypto-assets)	• Crypto-assets admitted or under application for admission to trading on domestic CASPs • Irrespective of trading venues (including transactions taking place on DEX and P2P transactions)		
(2) Material Facts	• Enumerating events that clearly constitute material facts, supplemented by a basket clause.		
	(i) Concerning the business or operations of the identifiable issuer	(ii) Concerning the handling of crypto-assets by CASPs	(iii) Concerning large-volume trades
	(Example) • Bankruptcy of the issuer • Discovery of significant security risks	(Example) • Commencement or discontinuation of handling a crypto-asset • Outflows of crypto-assets	• A decision to conduct, or to cancel, a transaction that would significantly affect the price of a crypto-asset (for example, transactions involving 20% or more of the outstanding crypto-assets)
(3) Insiders	Persons related to the issuer of a crypto-asset (including shareholders, administrative authorities, contracting parties)	Persons related to CASPs (including shareholders, administrative authorities, contracting parties)	Persons related to a large-volume trader (including shareholders, administrative authorities, contracting parties)
(4) Publication Measures	• Means of publication is limited to announcements made through the websites of CASPs or SROs. • Information dissemination via social media platforms is not regarded as a means of publication.*		
(5) Prohibited Acts/ Exemptions	• Engaging in "transactions", such as sale, exchange, or in-kind contributions, while knowing material facts that have not been published is prohibited. • The initial issuance of crypto-assets and corresponding initial acquisition are also prohibited. • (In addition to exemptions equivalent to those applicable to listed securities,) exempting the regulations where the person who engaged in the trade proved that the trade would have been executed even without knowledge of material facts.		

** This reflects concerns regarding the wide variety of platforms, the low level of dissemination of information among users, the ease of deleting and altering posted information, and the lack of assurance regarding the authenticity of the source and the content of information.*

Material 5: Strengthening the Functions of Self-Regulatory Organizations

(Source: Prepared based on page 41 of Material 2 for the 5th Meeting (Nov. 7) and page 7 of Material 2 for the 6th Meeting (Nov. 26) of this Working Group)

Strengthening the Functions of Self-Regulatory Organizations

Enhancement of Governance	• Strengthening financial and organizational foundations, including securing necessary human resources and increasing membership fee revenues, to achieve the following • Establishing appropriate governance structures and further enhancing neutrality and independence in reviews through establishing independent committees or organizations
Strengthening the review framework for crypto-assets: Commencement of handling and Disclosure requirement	• Enhancing review functions relating to the commencement of handling new crypto-assets (outsourcing part of the review process to highly specialized third parties should be permitted). • Enhancing review functions for disclosure items provided by issuers or CASPs (outsourcing part of the review process to highly specialized third parties should be permitted). • Strengthening information management and conflict of interest management frameworks, including measures to ensure that secondees from member firms do not engage in individual reviews. • Strengthening conflict of interest prevention measures, such as prohibiting the trading and holding of crypto-assets by officers and employees. • Strengthening monitoring and audit frameworks for CASPs
Strengthening Cyber Security	• Continuous improvement and strengthening of self-regulation, including initiatives to strengthen cybersecurity • Strengthening audit frameworks for CASPs
Strengthening User Protection	• Ensuring appropriate advertising and promotional activities by CASPs • Strengthening customer suitability assessments by CASPs (including ensuring the proper implementation of setting criteria for commencing transactions and limits on transaction amounts and holdings)
Measures against Market Abuse	• Establishment of a trade monitoring framework and substantial strengthening of market surveillance frameworks • Strengthening supervisory and verification functions relating to trade monitoring and related activities conducted by CASPs • Strengthening efficient and effective information sharing among CASPs, the SRO, and authorities

Material 6: Overview of Digital Asset Regulations (After the Review)

(Source: Prepared based on page 48 of Material 2 for the 5th Meeting (Nov. 7) of this Working Group)

Overview of Digital Asset Regulations (After the Review)

	Security Tokens	Crypto-assets: With an identifiable issuer — The issuer raises funds through the offering	Crypto-assets: Other crypto-assets — The issuer does NOT raise funds through the offering	Stablecoins
Legal Basis	The Financial Instruments and Exchange Act	The Financial Instruments and Exchange Act		The Payment Services Act
Disclosure Requirements	✓ Obligation for issuers to disclose upon commencement of handling and ongoing disclosure ✓ Obligation for FIBO handling security tokens to disclose information and provide explanations prior to the conclusion of a contract	✓ Obligation for issuers to prepare, disclose, and publish information, and to provide ongoing disclosure ✓ Obligation for CASPs to disclose information prepared by issuers	✓ Obligation for CASPs to prepare, disclose, and publish information, and to provide ongoing disclosure	✓ Obligation for issuers to disclose and explain ✓ Obligation for electronic payment instruments service providers handling stablecoins to disclose and explain
Business Regulations	✓ Application of regulations for Type I Financial Instruments Business ✓ Requirement to establish operational control frameworks appropriate for handling token-based products	✓ Application of regulations equivalent to Type I Financial Instruments Business ✓ Introduction of regulations under the FIEA tailored to the characteristics of crypto-assets		✓ Business regulations applicable to entities engaging in the trading, exchange, and custody of crypto-assets**
Market Abuse Regulations	✓ Prohibition of unfair trading and spreading of rumors ✓ Prohibition of insider trading for listed securities*	✓ Prohibition of unfair trading and spreading of rumors ✓ Prohibition of insider trading for crypto-assets handled by domestic CASPs		—

This table provides an overview of the regulatory framework applicable to digital assets. Certain exceptions may apply, and attention should also be paid to requirements under other applicable laws and regulations.

** Currently, no security tokens are listed on financial instruments exchanges*

*** Issuers are also subject to regulations under the relevant business laws (e.g., regulations applicable to funds transfer service providers), depending on the nature of the business they conduct.*