Web3.0 Research Group's Report

—Toward Sound Development of Web3.0

December 2022

Web3.0 Research Group

■ Members (Honorific titles omitted, in the Japanese syllabic order except for chairperson and vice chairperson, listed job titles are those presented at the time of institution of the Research Group)

Chairperson	KOKURYO Jiro	Professor, Faculty of Policy Management, Keio University
Vice Chairperson	INAMI Masahiko	Special Advisor to the President, Professor, Research Center for Advanced Science and Technology, The University of Tokyo
	ISHII Kaori	Professor, Faculty of Global Informatics, Chuo University
	ITO Joichi	Director & Chief Architect, Digital Garage, Inc.; Director, Center for Radical Transformation, Chiba Institute of Technology
	KAWAI Yuko	Representative Director CEO, Japan Digital Design, Inc.; Managing Director Head of Division, Mitsubishi UFJ Financial Group, Inc.; Managing Director Head of Division, MUFG Bank, Ltd.
	TONOMURA Keiji	Partner, Nagashima Ohno & Tsunematsu
	TOYAMA Kazuhiko	Group Chairman, Industrial Growth Platform, Inc. (IGPI)
	FUJII Taiyo	Writer
	MATSUO Shinichiro	Research Professor, Georgetown University
	YANAGAWA Noriyuki	Professor, Graduate School of Economics, The University of Tokyo

■ Meetings held (Honorific titles omitted)

Date of meeting		Agenda	
1	October 5, 2022	Discussion	
2	October 12, 2022	Hearing session	・ Nack Nao (shiftbase, inc.) ・ engineers [undisclosed]
3	October 21, 2022	Hearing session	・ KUSANO Emi ・ Digital Agency
4	October 25, 2022	Hearing session	・ NAKAJIMA Satoshi ・ Shiwa-cho, Iwate Prefecture
5	November 2, 2022	Discussion	
6	November 8, 2022	Study reporting	Contracted study (Note) interim report (1): Digital assets
7	November 18, 2022	Hearing session	・ TABATA Hajime (JP GAMES, Inc.) ・ HAYASHI Atsushi (Next Commons Lab)
8	November	Hearing session	・ MIYAGUCHI Aya (Ethereum Foundation)

	24, 2022	Study reporting	Contracted study (Note) interim report (2): Decentralized Identity (DID)
9	November 30, 2022	Study reporting	Contracted study (Note) interim report (3): Decentralized Autonomous Organizations (DAOs) User protection and Law enforcement
10	December 7, 2022	Hearing session	・ Financial Services Agency ・ Ministry of Economy, Trade and Industry
		Discussion	Summary of discussions so far (1)
11	December 13, 2022	Hearing session	・ Cabinet Secretariat ・ Cabinet Office ・ Ministry of Internal Affairs and Communications ・ Agency for Cultural Affairs
		Discussion	Summary of discussions so far (2)
12	December 23, 2022	Discussion	Finalizing the report

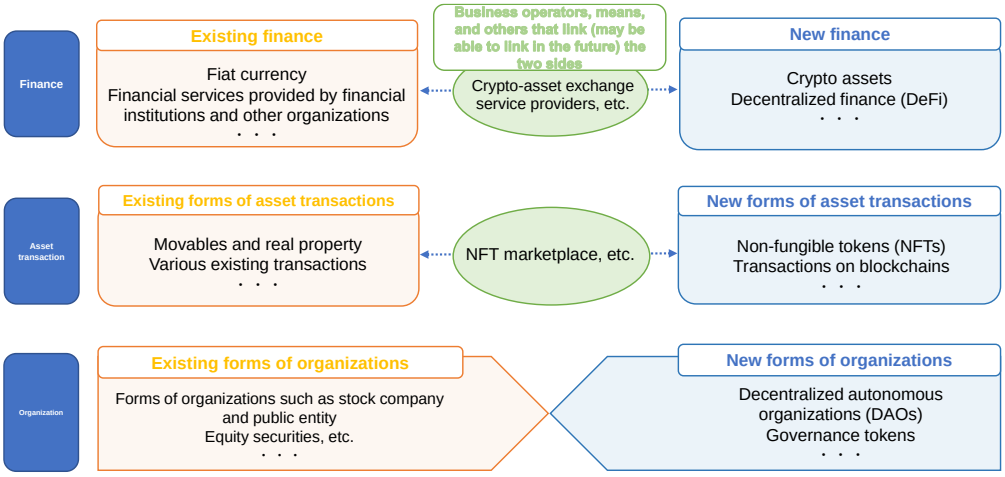
(Note) Outsourcee: Deloitte Tohmatsu Consulting LLC

1. General Arguments

(1). Background of and basic view in the discussions

Recent years have seen major global developments related to Web3.0, a decentralized application environment using new technologies, as well as worldviews built based on the environment. New services and tools have started to emerge for such elements as “finance,” “assets and transactions,” and “organizations” in particular, which are the core elements in economic society, and they seem to have the potential of technologically supplementing or replacing part of the roles played by existing services and tools.

The list of services and tools argued in relation to Web3.0 includes crypto assets, decentralized finance (DeFi), non-fungible tokens (NFTs), decentralized autonomous organizations (DAOs), and the metaverse, etc. These services and tools have different benefits, risks, and problems.



cf. In addition to the above, the metaverse and other technologies have emerged as a new space for activities.

There is no “silver bullet” technology for innovation, regardless of the technology. As such, even for new technologies discussed in relation to Web3.0, their potential for innovation should be considered after fully understanding what kind of technologies they are, what kind of problems they can solve, and what kind of risks they may pose that should be taken into consideration.

In addition, many of these new technologies may still be immature and require various trial-and-error before they can be used as solutions to

real problems. Accordingly, it should be understood that they will require a considerable period of time before they can be used as such solutions. Moreover, in order to realize the worldview built based on Web3.0 (refer to (2)), it is necessary to review not only technologies but also the market structures and systems themselves. For this reason, we have to say that the current situation is still far away from realization. As such, sound development of Web3.0 encompasses a broad range of points of argument in a “time frame,” which include a long-term future as seen in the discussion of ideal future form (refer to (3)) and imminent measures which need to be taken for issues related to systems and regulations (refer to (4)) and measures to promote innovation (refer to (5)). Therefore, “time frame”-oriented discussions are always necessary.

As seen above, while it is not certain how individual technologies, services, and tools develop in the future, it is reasonable to assume that they will have some influence on the global economic society. In Japan as well, it is expected that the content industry and local communities will be revitalized through co-creation in the form that has not been seen before, which is produced by mutual connection of individual elements. In addition, contribution by Japanese companies in the protocol layer, which is the basis of technologies, is also expected. Under such circumstances, the Research Group’s basic view is to use new digital technologies underlying Web3.0 as tools to solve various social problems and realize Japan’s economic growth. Based on this basic view, the Research Group examined how to create an environment to promote Web3.0.

The results of discussions by the Research Group on the following points are summarized in 2 and onward.

2. Digital assets
3. Decentralized autonomous organizations (DAOs)
4. Decentralized identity
5. Connection with metaverse
6. User protection and law enforcement

The risks and problems discussed by the Research Group are important issues that we must face to realize the ideal future form of Web3.0. In areas where innovative advances have been made, such

as the Internet and finance, there is a history in which we have overcome various problems we have faced through technology development, R&D, and the improvement of regulations and services. We hope that the discussions by the Research Group serve as an opportunity to steadily push forward efforts for the sound development of Web3.0 in the future, without being flinched by these problems.

(2). Direction of the discussions

The main feature of the worldview built based on Web3.0 is a possibility in which innovative services emerge more rapidly than ever before through markets with no barriers to entry which are realized through public blockchains and smart contracts which have been built as open source software to enable everyone around the world, beyond borders of countries and organizations, learns from each other, promotes technological innovations by inspiring each other, and repeatedly makes trial-and-error efforts by freely combining publicly available components. It is desirable that we make the utmost use of such feature toward sound development of Web3.0.

The possible approaches in the discussions would be to envision the ideal future form of Web3.0, and to consider how the current systems should be changed to make a transition toward the form and how the current systems should be reviewed as the precondition to enable such change.

In so doing, from the viewpoint that the more essential the innovation is, the less likely it is that we know what will happen in the future, it is important that diverse human resources share certain principles and lead innovation by promoting creation of new things, without fixing the ideal future form.

In the Web3.0 world in particular, technologies and business environments change quickly, and existing regulatory systems do not fit in many aspects. Accordingly, a technique to quickly respond to changes in the environment and bear results, called the “OODA (Observe, Orient, Decide, and Act) Loop,” seems effective. Using this and other techniques, we will create a system in which diverse human resources think and act on their own initiative, their thoughts and actions are organically combined, and better services and tools are selected. By so doing, we aim to develop and bring human resources,

who take charge of innovations, in and into Japan.

(3). Ideal future form of Web3.0

There is a concept of seeking the ideal form of Web3.0 in connecting individual elements in a decentralized way, using technologies including blockchains. New worldviews are expected to be created through space expansion, which is realized through intersection of the virtual space called metaverse and multiverse and the real world.

More specifically, the connection of individual elements will generate a new form of co-creation, and efforts to immediately and appropriately establish an environment for intellectual property including how we make secondary use of such intellectual property is expected to create new value and accelerate innovations. Establishment of such an environment is expected to allow younger generations to participate in society without barriers and play an active role in a global field in the future, and also result in solution of social problems that has been difficult to achieve in the past.

In addition, they have the potential to generate significant economic value, particularly in the cultural and economic areas (such as content, games, arts, and sports) which Japan has strengths. It is expected that the use of tokens such as NFTs and fan tokens enables securing of additional revenue sources for IP holders, creators, and other stakeholders, retention of loyal fans, and in turn, revitalization of industries in the cultural and economic areas. It is also considered important to create an environment where such Japan’s strengths can be developed in the near future.

Furthermore, the metaverse has now made possible the distribution of intangible objects whose value was difficult to determine. Thus, the form and means of distribution of value have been changing. It is expected that, through such developments, communities which have been increasingly divided along with the development of information and communication technologies are to be connected in the near future and create new value, once again.

Ultimately, there is the possibility that in the future the concepts of individual and freewill may change, as seen in cases where an individual person may use multiple bodies or multiple persons may share one body; under such circumstances, value, ownership, and

transactions may be redefined.

Various and repeated trial-and-error efforts toward realization of new worldviews will result in breakthrough of technologies and how we use such technologies, as well as changes in existing industries and organizations in response to various inspirations. This fact itself has value, and it is important to immediately provide support for engineers and creators who will be actors in such changes.

(4). Issues related to systems and regulations in realizing the ideal future form

In the Web3.0 world where technologies and business environments change quickly, from the perspective of promoting innovations, it is important to clarify the areas controlled by hard laws, consider how we should form flexible rules including soft laws, and immediately create a mechanism in which related parties repeatedly verify and revise the rules on a periodic basis. It is also important that the mechanism is accepted by society.

In the Web3.0 world where cross-border activities are common, it is important to build globally accepted rules and consensus, instead of taking classic approaches of national laws and multilateral conventions. As the prerequisite, it is also important to have a viewpoint of ensuring the comparability of regulations of different countries.

On the other hand, as detailed below, there is a growing area for blockchain-based services and tools that is difficult to control by laws and regulations alone, which points to the necessity of reconsidering their enforceability and the role of regulations.

(i) Decentralization results in the absence of intermediaries and the ownership of responsibility and the targets of regulations related to provision of services and tools become obscure.

(ii) There is a possibility that services and tools cannot be suspended due to their autonomy despite intervention by regulatory authorities.

(iii) There is a possibility that the traceability by regulatory authorities will be lost due to the anonymity.

(iv) There is a possibility that after-the-fact corrections may become difficult despite intervention by regulatory authorities, due to the impossibility of modification or deletion of records without consent of network participants due to the tamper resistance.

(v) Due to the openness, the ownership of responsibility becomes unclear because it becomes an environment where anyone can develop and participate without permission.

To address these problems, just like we did in the Research Group, it is necessary to effectively and efficiently operate a mechanism to share the latest awareness of problems among members and related ministries and agencies at all times and cooperate in addressing the problems. Concrete action needs to be taken immediately.

In addition, there are global opportunities for all stakeholders including the academia, engineer, business, and regulatory authorities to deepen the common understanding of the current situations and hold discussions from an open and neutral standpoint to work on issues faced by them in a collaborative manner (such as the Blockchain Governance Initiative Network (BGIN)). Such opportunities have been pushing forward with global and leading discussions on some of the topics which the Research Group have discussed. Concrete actions need to be taken immediately so that stakeholders in Japan access such opportunities more actively and work to solve issues through global collaboration.

(5). Measures to promote innovations

To create new value and accelerate innovations, it is considered important to create an environment which allows for various challenges in the Web3.0 world as well. Related ministries and agencies need to take the following measures steadily as part of urgently required measures to promote innovations.

(i) Platforms as a venue for dialogs

As a venue for dialogs between municipal governments and related ministries and agencies, the Web3.0 Information Sharing Platform was established under the “Digital Reform Co-creation Platform” on October 7, 2022. The platform promotes information exchange related to the status of studies by the Government and examples of leading-edge initiatives undertaken by municipal governments, among other things, as well as sharing of issues of mutual interest.

In addition, dialogs will be held occasionally with business operators, etc., with whom we have contacted through industrial associations,

using easily accessible online tools.

(ii) Establishing of "consultation desk," and holding of the "liaison meetings for related ministries and agencies" to solve issues

The Digital Agency, which serves as a consultation desk regarding individual and specific issues faced by municipal governments, business operators, and other stakeholders, collects information on such issues making use of the channels including the above platform and takes action in collaboration with related ministries and agencies. The liaison meetings for related ministries and agencies will discuss and work out any issues that cannot be solved immediately.

(Note) Municipal governments include those that are working on digital implementation making use of the "Vision for Digital Garden City Nation Subsidy."

(iii) International information provision and involvement in consensus formation in relation to Web3.0

Related ministries and agencies will provide support for Web3.0-related events including international conferences sponsored by the private sector as well as support for appropriate information provision so that Japanese companies, human resources, and other actors can have contact with international Web 3.0 players to realize collaboration, recruitment, fund-raising, global expansion, and other initiatives, as well as to attract human resources that will take the lead in innovation into Japan. In addition, it is important for Japan to participate in discussions to build global consensus. In doing so, it is important for the government to provide information focusing on the social and economic benefits that Web3.0 can bring about, not focusing on specific operators, businesses, or services.

(iv) Development of principals in R&D and technology development

Toward the sound development of Web3.0, it is essential to build a decentralized application environment which serves as the basis therefor and to have and develop a thick layer of the academia and engineers who will be the principals of innovations of infrastructures and services built thereon. For this reason, related ministries and agencies need to take the following measures immediately.

- Discovery and development of human resources who have creative ideas and technologies to generate innovations as well as excellent abilities to utilize such ideas and technologies, and who are expected to play a leading role on the global stage
- Discovery and development of the following human resources to expand the base for making trial-and-error efforts toward sound development of Web3.0:
  A) Human resources who can design safe protocols
  B) Human resources who can design safe software and hardware
  C) Human resources who will be the principals of operations that can withstand various attacks and incidents
  D) Human resources who can play a role in government relations in normal times and in cases of emergency

The U.S. Executive Office of the President announced the measures for promoting responsible innovations (September 2022). The following points in particular will be helpful when considering measures to promote innovations in Japan.

- Formulation of the “Digital Asset R&D Agendas” and commencement of basic research on matters such as next-generation cryptology, transaction programmability, cybersecurity, privacy protection, and mitigation of an impact of digital assets on the environment (Office of Science and Technology Policy and National Science Foundation)
- Support for research on social science and education to develop methods to provide information for, educate, and train diverse stakeholders on safe and responsible use of digital assets (National Science Foundation)

As described in (2) above, the main feature of the worldview of Web3.0 is that everyone around the world, beyond borders of countries and organizations, learns from each other, promotes technological innovation by inspiring each other, and repeatedly makes trial-and-error efforts by freely combining publicly available components. This feature is in common with the essence of R&D and technology development. It is expected that human resources in the culture and economic areas, which are the strengths of Japan, will play a role in the foregoing to

create new value unique to Japan. Moreover, as stated in (4) above, stakeholders' collaboration on a global scale is becoming increasingly important. From the perspective of developing Japan's academia and engineers, it is necessary to create an environment which allows such people to actively participate in various forums including the BGIN and to obtain timely exposure to cutting-edge global discussions and knowledge.

(6). Future initiatives toward sound development of Web3.0

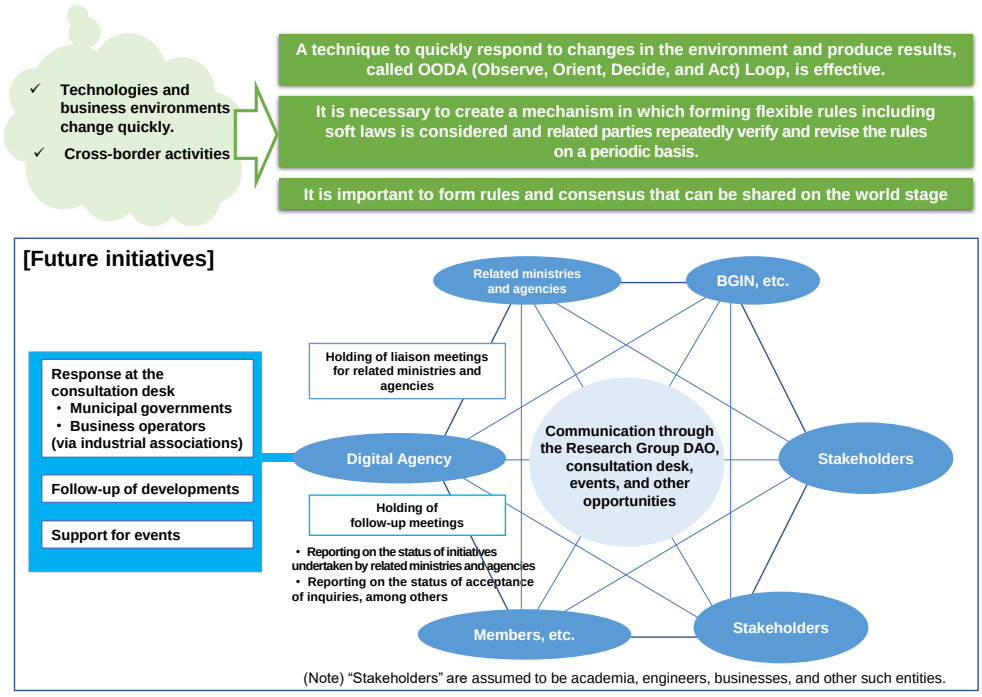
The main focus of the discussions by the Research Group has been centered around the possibilities and problems of the decentralized application environment which uses new technologies, called Web3.0, as well as worldviews built based on the environment. Based on such discussions, arguments described in 2 and onward provide a basic direction for sound development of Web3.0, resting on current awareness of problems.

In the Web3.0 world, technologies and business environments are changing rapidly, and existing regulatory systems do not fit in many aspects. Accordingly, in addition to handling of individual issues by related ministries and agencies, as we did in the Research Group, it is necessary to effectively and efficiently operate a mechanism to share the latest awareness of problems among members and related ministries and agencies at all times, and to cooperate in dealing with the problems.

Based on the discussions by the Research Group, the Digital Agency aims to create an environment where various challenges may be taken up without unreasonable barriers through the establishment of the consultation desk, as well as the holding of liaison meetings for related ministries and agencies to solve problems.

In addition, assuming that the Web3.0 Research Group DAO (refer to 3(2)(ii)), which was established based on the discussions by the Research Group and whose initial members are the members of the Research Group and others, will continue and develop autonomously in the future, it is desirable for said DAO and related ministries and agencies to work together, and for Japanese stakeholders to proactively participate in collaborative efforts such as the BGIN to solve global problems.

Based on such an open architecture, we aim to broaden the base of actors who work on sound development of Web3.0, to allow diverse human resources to think and act on their own initiative under the “OODA Loop,” and to organically combine them so that more reasonable systems and better services and tools are selected.



2. Digital assets

While digital assets have the potential to bring new benefits through the use of various tokens, a variety of issues are pointed out from various perspectives including user protection. It is necessary to swiftly solve issues that are said to be the current barriers for Japanese business operators in handling tokens. It is also necessary to follow up ongoing global arguments on such matters as user protection and the prevention of financial crime. It is also necessary to respond to issues related to transactions of non-fungible tokens ("NFTs") which are used in various forms, while sorting out issues related to the applicability to crypto assets and rights represented by NFTs. In responding to such issues, as this is an area where the framework for regulations is rapidly changing globally, the discussion should be held based on global trends, without unnecessarily prioritizing domestic regulations only. Response needs to be taken flexibly so as to cope with future environmental changes. In addition to these considerations, NFTs in particular have the possibility of supporting creators and content which are the pillars of the cultural and economic industries. Accordingly, in addition to the above discussions, it is important to have the perspective of developing the industries themselves. Accordingly, it is necessary to ensure the reliability of NFTs and appropriately protect creators and content on NFT platforms. Response to security issues is also a precondition for sound development of Web3.0. Also required is support for private-sector initiatives toward retention and development of human resources.

(1). Digital assets and discussions thereon

Under the decentralized application environment leveraging new technologies, digital assets, which enable digital expression of value and rights, are seen to have the potential of bringing new benefits that have never been seen before. More specifically, the focus is on the possibility of their ability to add functions, in which holders see a variety of value and benefits, to tokens. This is expected to give birth to new types of business activities and models, leading to the solution of social problems and economic growth in the future. Above all else, they have the potential to generate significant economic value in the cultural and economic areas (such as content, games, arts, and sports) in particular, where Japan has strengths. It is expected that the use of tokens such

as NFTs and fan tokens enables securing of additional revenue sources for IP holders, creators, and other stakeholders, retention of loyal fans, and in turn, revitalization of industries in the cultural and economic areas.
In order to create an environment where such expectations come to life, the Research Group, with a belief that it is required to steadily push forward with initiatives to solve various problems currently recognized, examined the points of argument described in (2) and thereafter.

The Research Group held discussions by largely categorizing digital assets into the three categories ((i) through (iii)), as shown in the table below. Digital assets are related to all of “finance,” “assets and transactions” and “organizations” listed in 1, and have the multi-layered correspondence with (i) through (iii). For example, the system development in the “finance” field has been making progress for (i) and (ii), while governance tokens are related also to “organizations.” As NFTs continue to be more diversified, (iii) may have a relationship with any of “finance,” “assets and transactions,” and “organizations,” depending on the actual situation of transactions and rights represented. In addition, it is possible that the categories may vary depending on the circumstances of the use in the future. However, as described below, while international discussions are expected to make progress in areas of (i) and (ii) in the future with the aim of protecting investors and establishing the reliability, toward the sound development of Web3.0, in the area of (iii) in particular, it seems important to establish an environment which enables Japan to generate use cases for value creation ahead of the world.

Digital assets	(i) Crypto asset (virtual currencies)	2008: Advent of blockchain technologies and Bitcoin → A system of registering exchange service providers was introduced (the Payment Services Act was amended in 2016)
	(ii) Security token	Funds were raised using tokens → Regulations such as those on disclosure and those on sale and solicitation were established (the Financial Instruments and Exchange Act was amended in 2019)
	(iii) Diverse tokens other than the above	Various types of tokens including NFTs linked with content became increasingly common

In Japan, among digital assets, crypto assets and security tokens (securities for which the transfer and recording of rights are carried out

using an electronic data processing system such as blockchain technologies) are handled within the financial legislation. In various other countries as well, there are cases where digital assets are handled within the framework of their respective financial legislation. In November 2022, a leading global crypto asset exchange went bankrupt. Triggered by this event, the momentum for international discussions on such matters as governance and investor protection is growing. Under such circumstances, it seems that actions toward establishing the long-term reliability of the ecosystem surrounding digital assets continue to be necessary.

NFTs and such other tokens are believed to be not qualified as crypto assets and security tokens, in principle. Regarding these tokens, issues such as the following have been pointed out: creators who hold rights in the content represented by NFTs and such other tokens are not protected; the criteria for determining the applicability to crypto assets are not clear; NFT issuers may not always be the holder of rights related to the content; there are many cases in which security related to content is not guaranteed; and there is a concern about them being used for money laundering. The nature of NFTs themselves is diverse. Therefore, it is necessary to consider how they should be positioned in laws, regulations, and other rules and how other various issues should be dealt with individually and specifically. On this point as well, appropriate actions including provision of support in the formulation of guidelines by business operators and industrial associations seem necessary, while taking developments in international discussions into consideration.

While points of argument regarding digital assets are not limited to the above and there are various details and points of argument that require discussions, the Research Group held discussions mainly on the following matters. Refer to [Reference 3] regarding the overview of domestic and international discussions on digital assets.

(2). Main matters discussed by the Research Group and direction of actions

(i) Discussions on digital assets used as a means for fund-raising

Regarding fund-raising through issuance of tokens, it is said that functions may be added to tokens in which holders see a variety of value and benefits. At present, issues when Japanese business

operators handle tokens have been pointed out as follows.

- For companies using blockchain technology in Japan, taxation using the term-end market value of crypto assets is a factor hindering business development.
- Venture capital companies cannot invest in the token business using the investment limited partnership (so-called LPS) because obtaining of tokens and similar businesses are not covered as businesses subject to the LPS.
- There are cases where audit firms refuse to undertake accounting audit of business operators handling tokens for reasons such as that, while the sufficient establishment of internal control and governance is the prerequisite for audit, the business operators have not sufficiently established internal control and governance.

While related ministries and agencies are considering actions on these issues, the prompt solution of the issues is required as it is the precondition for establishing the business environment toward sound development of Web3.0.

On the other hand, it is also pointed out that the high level of risk needs to be fully recognized which arises when domestic and foreign parties such as venture capital companies, which may find it difficult to raise funds from so-called professional investors, widely raise funds from general investors through issuance of tokens in overseas countries, under the circumstance in which the framework for investor protection has not been established.

In the meetings of the Research Group, the following opinions were presented regarding digital assets used as a means for fund-raising.

- In light of ae large number of fraudulent cases, at present, careful consideration should be paid to the possibility.
- Detailed consideration on benefits and risks is required, in reference to actual cases, comparing with existing means for fund-raising (for example, initial public offering (IPO) and security token offering (STO) based on the Financial Instruments and Exchange Act).

In addition, there are tokens, which are not qualified as crypto assets and security tokens, issued for fund-raising for organizations, and such

tokens may be significantly affected by the financial position and information of the issuer. Despite this fact, unlike securities under the Financial Instruments and Exchange Act, there are no regulations on information disclosure, insider trading, and market manipulation for such tokens. This is also recognized as a problem.

Based on these discussions, it is deemed necessary to consider the issues from the various perspectives including consumer protection, financial stability, and the prevention of financial crime, while analyzing (1) what functions are specifically added to tokens and what value and benefits are seen by the token holders, and (2) in what points fund-raising through issuance of tokens is beneficial as compared with the existing means for fund-raising.

(ii) Summary of legal position of NFTs

A. Basic nature of NFTs and the possibility of use as a payment method

NFTs are used in various forms, including the areas of art, collectibles, items, and certificates. The definition and category are also various by country and region. NFTs are basically electromagnetic records which are uniquely identifiable in distributed ledgers. The legal nature should be governed by the nature of rights which the NFTs represent and circumstances of transactions. Consequently, it is difficult to uniformly define NFTs as being legally equivalent to something.

For example, Ethereum offers different standards for tokens, including ERC-20, which records the remaining balance, ERC-721 (non-fungible token), and ERC-1155 (semi-fungible token). There are cases in which series of ERC-721-based NFTs are traded at the same price. Therefore, it is difficult to uniformly determine whether it has the nature capable of being used as a payment method based on their technological specifications.

Regarding this point, an opinion was raised at the Research Group that it is important to sort out the applicability of NFTs to crypto assets, because some NFTs have functions as a payment method and accordingly may be qualified as crypto assets under the Payment Services Act. Similar discussions are going on in the U.S. and Europe on this point (see [Reference 3] B). The competent ministries and

agencies plan to formulate guidelines for interpreting whether tokens including NFTs may be qualified as crypto assets in the future.

B. Categorization according to rights represented by NFTs

Rights that may be represented by NFTs include, for example, various rights related to content, rights to use items in games, rights to vote in organizations and projects, rights to receive services, rights to use real property, membership rights, and other types of rights.

Regarding this point, it was pointed out at the Research Group that, for example, if NFTs are sold on platforms, the rights and interests shall be governed by the terms of use of the platforms; however, currently, rights represented by NFTs are not always clearly stated in the terms of use, and the treatment of rights is left obscure.

It was also pointed out that tokens with various functions have names that are not always clearly relevant to their functions. For example, a token that is said to be a governance token may actually be distributed as a security token as it is added with functions other than participating in decision-making of an organization (such as profit-making functions). Based on the foregoing, an opinion was raised that, from the perspective of user protection, it is necessary to consider how tokens' names should be in terms of the relevance with their substantial functions.

NFTs that may represent various rights may be further used in diverse forms in the future. Taking the above points into consideration, it is necessary that related ministries and agencies governing the systems, depending on the rights represented, work to understand the actual circumstances and take necessary actions for appropriate protection of rights of related parties and other such matters in reference to issues and points of argument indicated in [Reference 2].

C. Recognition of users concerning NFTs

The value of NFTs that may represent such matters as art, collectibles, and items may not be uniquely determined by fungible monetary indicators. Instead, the value may be determined by the characteristics

unique to the tokens including the content represented by the NFTs and the benefits provided to the holders of such tokens.
In the meetings of the Research Group, the following opinions were presented as the points of attention when considering the legal position of NFTs.

- New problems may arise if the legal position of NFTs deviates from users' recognition. Investigations and examinations are required for not only legal position but also users' recognition.
- For example, for NFTs that represent digital art, the viewpoint of art collectors is required, instead of focusing on the similarity with securities and crypto assets.

Similar awareness of the problem is observed in discussions in the draft Regulation on Markets in Crypto Assets (MiCA) in Europe, where the value of tokens is discussed from not only the perspective of the value as payment method but also subjective value in ownership.
In considering the legal aspects of NFTs in the future, discussions may need to include not only outer rights and interests but also subjective points as to what value is seen in NFTs by users.

(iii) Issues related to transactions of NFTs

NFTs are less liquid than crypto assets (fungible tokens) which are generally widely distributed and can be used as a payment method. NFTs are susceptible to the impact of insider information held by issuers and/or marketplaces, and thus are characterized by the susceptibility to price manipulation.
NFTs may be widely used as a means for fund-raising. On this precondition, it is necessary to consider, on an as-needed basis, anti-money laundering/countering the financing of terrorism (AML/CFT), the necessity of disclosure, risks of them being used for insider trading, market manipulation, wash sale and other fraudulent acts, and how the regulations should be, while paying attention to global developments including establishment of systems and enforcement of laws in various countries and international discussions on frameworks, and also striking the balance with promotion of innovations.
In addition, many of the NFTs are traded in cross-border transactions, and there is a limitation in regulating them within Japan in advance. In

considering how regulations should be, it seems important to contribute to international discussions held by such parties as the Financial Action Task Force (FATF), while collecting information on an ongoing basis to take flexible actions for understanding actual circumstances and providing information to prevent user damage in Japan.

(iv) Necessity of protecting creators and content

A. Ensuring the reliability of NFTs

It is deemed important to protect content linked with NFTs and creators who create them. While it is said that not a small number of items traded on the world's largest NFT platforms are fakes, a request was made from one of the parties we had hearing sessions with that certification programs by organs such as government agencies be considered to ensure the reliability of NFTs.

An opinion was raised from a member of the Research Group against the request, stating that the worldview of Web3.0 is grounded in global and permissionless innovations, which is inconsistent with the request, and therefore, the ideal ecosystem to be created might be a system led by users and markets.

In order to ensure the reliability of NFTs, the necessity of measures such as the following has been pointed out: certification of wallets and contracts under which NFTs are issued, disclosure of information on rights represented by NFTs (including license to use content and whether there is a contract regarding secondary distribution), measures to preserve the status of the infringement of rights including use of NFTs that represent content without obtaining a license from the right holders (unlicensed NFTs), and a penalty for issuers and purchasers of unlicensed NFTs. On this point, specific actions are being taken by private sector groups. Related ministries and agencies are required to continue providing support for such private sector groups and provide appropriate information to users.

B. Terms of use of NFT platforms

An opinion was presented stating that, even in Web3.0 whose ideal vision is the connection of individual elements rather than centralization, transactions have already been overly concentrated in NFT platforms, and as a result, there is a concern that it has become a system in which

profits of platform business operators are pursued rather than placing a focus on the perspective of creators who have rights in content represented by NFTs.

More specifically, it was pointed out that it is difficult to realize creator support, which is one of the benefits users place a particular focus on in NFTs, in NFT platforms which make creators who are the authors of works represented by NFTs to waiver the copyrights in their works and receive no royalties associated with the use of works. How the terms of use of NFT platforms are stipulated is an important point of argument in considering protection of content and creators.

It was also pointed out that, in the Web3.0 worldview, legal disputes may arise on a global basis, and therefore, it is necessary to consider how dispute resolution means should be designed.

With regard to problems related to terms of use of NFT platforms, while it is possible that creators and content are not appropriately protected depending on the terms of use of NFT platforms (e.g.: royalties for creators are not sufficiently provided), existing legislation may act as a check (for example, if a platform business operator, whose own position in transactions is superior to that of creators, unilaterally raises commissions by changing the terms of use, unfairly and disadvantageously to creators in light of normal business practices, it may have the risk of being considered as an abuse of the superior position, which may be a problem under the Antimonopoly Act.). The deepening of discussions is expected in the future as to whether the issues should be solved through competition among platforms under the market principle, or whether certain disciplines should be established by sorting out responsibilities and roles of platform business operators. In addition to aforementioned initiatives to ensure the reliability of NFTs, actions of related ministries and agencies based on international discussions concerning how NFT platforms should be are required..

C. Importance of provision of information to creators

In Japan, there are a large number of creators who can create high-quality content. Despite this fact, some of them are not fully taking advantage of new digital tools including NFTs. It was pointed out that, in order to produce creators who can play an active role on the global

stage in the future, it is important to support creators by providing them with appropriate information, including the benefits and risks of using these tools.

In light of such circumstances, related ministries and agencies are required to take measures to support creators, including provision of information necessary from the perspective of creators, based on their awareness of issues.

(v) Discussions on security

It was pointed out that, at present, similar services derived from existing services are provided without receiving security verification, and a large amount of funds are said to be collected by such services and then leaked. Response to security issues is a precondition for sound development of Web3.0.

In the meetings of the Research Group, the following opinions were presented on security.

- Incidents such as leakage of digital assets to the outside caused by unauthorized access damage the reliability of the entire Web3.0 ecosystem. Therefore, it is necessary to address security issues by sharing information among relevant organizations in a timely manner.
- Based on the framework of risk management systems cultivated to date, by analyzing risks that could additionally arise in Web3.0, necessary human resources should be sorted out to address them.

As for security, the U.S. has formulated digital asset R&D agendas including actions on cybersecurity, commenced basic research, and developed action policies on the safe and responsible use of digital assets.

Japan also faces the important issues of securing and developing human resources who take action on security in Web3.0. Related ministries and agencies are required to continue providing support for private sector initiatives to secure and develop human resources.

(3). Basic direction of sound development of Web3.0

Among the points of argument regarding digital assets, the Research Group held discussions mainly on the points as to whether they can be a means for fund-raising in particular, what are the issues of tokens

which are not qualified as crypto assets and security tokens, and how these issues should be sorted out.

The specific problems recognized regarding tokens are discussed in items (i) through (iii) in (1), based on the discussions by the Research Group as well as various issues pointed out from the event that a leading global crypto asset exchange went bankrupt in November 2022.

NFTs in particular have the possibility of supporting creators and content which are the pillars of the industry. Accordingly, in addition to the above discussions, it is also important to have the perspective of developing the industry itself, without being focused only on their problems.

As seen in the above, although they are all called digital assets, respective points of argument significantly differ among them, depending on the functions they have and content they represent, among other things.

It is necessary to consider the framework for regulations based on risks pointed out concerning the issues of user protection in digital asset transactions, and initiatives to ensure the reliability. Regarding this point, attention needs to be paid to avoidance of hindrance to market growth, while appropriately giving consideration to user troubles and problems regarding protection of creators' rights caused by market growth. In so doing, as this is an area where the framework for regulations is rapidly changing globally, discussion should be held based on global trends, without unnecessarily prioritizing domestic regulations only. Responses need to be taken flexibly so as to cope with future environmental changes.

3. Decentralized autonomous organizations (DAOs)

Decentralized autonomous organizations (“DAOs”) use blockchain technologies and smart contracts, do not have central management structure, and aim for autonomous operation by participants. This form of organizations is expected to be a new way of governance that could have never been realized in the past. Some assert that they can replace the existing organizational form of a stock company. However, the current situation is that philosophy is ahead of the accumulation of actual cases to discuss them more specifically. While it is understood that there is no internationally unified understanding or definition of DAOs, there are many organizations with various purposes and functions are operated as DAO. Globally, there are cases where they are used as a tool to collect a large amount of funds while circumventing the application of laws and regulations. Under the circumstances, in Japan, the focus is on the use of DAOs for activities such as local community revitalization and supporting artists, the main purpose of which is not for profit. First and foremost, shared understanding needs to be established on such matters as what governance or incentive mechanism is desired to be incorporated into such activities and what is the significance of selecting the organizational form of DAO. To this end, an important issue to be considered is how we create an environment that allows for various trial-and-error efforts. A consultation desk established by the Digital Agency needs to conduct ongoing follow-ups in collaboration with related ministries and agencies so that initiatives toward the realization of expectations for DAOs, such as solution of social issues and creation of new value, are implemented appropriately, while obtaining shared understanding of issues surrounding initiatives related to DAOs. In so doing, it is also important that technological issues including security are not discussed within closed circles related to individual DAOs, but rather, measures are considered so that limited human resources are efficiently used by, for example, sharing best practice.

(1). DAOs and discussions thereon

The important things in the sound development of Web3.0 are to build a necessary business environment which enables the solution of social issues and value creation and to consider measures to protect users,

with an eye on benefits and risks that may be brought about through a new form of personal and economic ties created by the use of DAOs.
To this end, it is important to analyze the actual circumstances of DAOs in Japan and overseas from multi-faceted aspects including technology, economy, and governance and sort out their benefits and issues, while sharing experience of use by the Web3.0 Research Group DAO and providing standard infrastructures and tools.
From this point of view, the Research Group held discussions mainly on the following matters. Refer to [Reference 4] regarding the overview of discussions related to DAOs.

(2). Main matters discussed by the Research Group and direction of actions

(i) Positioning of DAOs

DAOs are organizations characterized by autonomous operation by participants, without a centralized management structure. In general,, the term DAOs refers to organizations which are based on blockchain technologies, smart contracts, and other software-based systems.
Regarding this point, it was pointed out that, as the degree of decentralization is relative, the nature of organizations may become clearer if the degree of decentralization is considered from the perspectives such as the technological perspective including protocol design, the economic perspective including wealth distribution design, and the governance perspective including decision-making of organizations.
It was also pointed out that the essence of DAOs lies in the smart contract system playing a central role. Under the system, how funds are used is decided by a majority vote.
At present, how decentralized and how autonomous DAOs can be are not clear. A document published by the U.K. Law Commission (Decentralized autonomous organizations (DAOs) Call for evidence, dated November 16, 2022) states that, assuming DAOs as organizations that rely on blockchain systems, smart contracts, and other software-based systems, there is no unified understanding and definition of DAOs, and positions a DAO as a new type of technology-mediated social structure or an organization of participants.
The term DAOs herein refers widely to organizations which have a purpose of increasing the degree of decentralization and autonomy by

generally using blockchain technologies, smart contracts, and other software-based systems.

(ii) Purposes of establishment of DAOs and priority of discussions according thereto

DAOs are established and operated for various purposes, and it is said that those that manage software protocols including decentralized exchanges as well as related tokens top the list in terms of the global aggregate market value. On the other hand, there are various types of DAOs including those whose purpose is to contribute to society by way of donations and other means, without pursuing profits.

At the Research Group, questions were posed on what specific benefits for community management have been brought about by technologies such as blockchain technologies and smart contracts, which are considered to be utilized by DAOs, and what specifically cannot be achieved through incentive mechanisms based on existing legal systems and communication tools. Further discussion is needed to promote a common understanding of the social importance of DAOs.

The legal position and social significance of DAOs are deemed to vary depending on their purposes and nature. In Japan, emphasis has been placed on DAOs which aim to solve social issues such as community revitalization or to support artists, whose main purpose is not for profit (meaning profit-making activities through operation of an organization and distribution of such profits to members). As such, there was an opinion stating that we need to consider what should be given priority in the examination.

Against the backdrop of these ideas, as seen in the following opinions, it is considered important to share deepened understanding of the benefits and problems through the operation of a DAO whose main purpose is not for profit.

- It may be good if, by actually operating a DAO, discussions could be deepened on how to prevent the “tragedy of the commons” (shared resources which can be used by anyone are damaged or depleted due to excessive consumption and other reasons) by incorporating what kind of governance and incentive mechanisms

into activities, the main purpose of which is not for profit, and the outcome be shared by various communities.

- More specifically, we could operate the Research Group itself as a DAO and share the specific experience regarding benefits and problems. By so doing, it can be expected that our experience will serve as reference for future initiatives by organizations such as municipal governments, and that an increased number of engineers come into contact with Web3.0 if we publish our regulations and codes as open source.

(iii) Expectations for DAOs and direction toward realization thereof

What are expected of DAOs include the potential for DAOs to (1) get many diverse people involved in activities globally; (2) prevent the tragedy of the commons by aligning interests of participants; (3) enable fair and efficient organization management by using smart contracts; and (4) ensure fairness by taking advantage of high transparency based on blockchains.

Major opinions on expectations in Japan and the direction of how such expectations are realized included the following.

- If bottom-up initiatives in which local communities realize their new ideas through DAOs increase and various issues are solved through participation by not only human resources who are working on local issues but also human resources who have specialized skills in areas such as technology, economy, and governance, such initiatives may serve as a turning point for Japan in creating a lot of human resources who can play the role of rule maker on a global scale.
- It is important to have discussions from the viewpoints of how optimal governance should be established in the community of DAOs and how human resources who can create a society where social issues are solved through activities of DAOs should be supported.
- It is desirable to refine discussions on whether DAOs are for communities or for society through the pursuit of conditions for communities that work as bottom-up-type DAOs, connection of multiple DAOs, and connection of DAOs with society.

(iv) Various issues surrounding DAOs and actions to be taken

As issues surrounding DAOs, it was pointed out that (1) DAOs may be abused for circumvention of regulations and for criminal acts because the ownership of responsibility is unclear; (2) obtaining consensus is difficult when people are lightly involved under anonymity; and (3) legal systems are not keeping pace with the development, and DAOs do not have legal personality in general, and therefore, DAOs face limitations in conducting transactions such as entering into contracts.

At hearing sessions, the following were pointed out as issues regarding DAOs in terms of economy and governance.

- Issues in terms of economy: There have been no successful cases of token economics where profits are appropriately distributed, and cases which were believed to be an excellent system actually have collapsed. It is not certain whether we can actually harness token economics.
- Issues in terms of governance: Even in non-profit DAOs which use public blockchains, there have been cases where communication among people broke down when deciding how the funds collected should be used by a majority vote, as factions were formed within the organization and the organization was internally divided pursuing the acquisition of such funds.

In the meetings of the Research Group, the following opinions were presented regarding governance.

- The spread of attempts to use governance tokens for consensus building is favorable from the perspective of realization of digital society. It may be significant to analyze the possibility of more efficient consensus building using AI.
- Smooth communication using technologies can be realized without taking the form of DAO. It is difficult to find rational grounds that DAOs enable alignment of interests among related parties. There seem to be illogically excessive expectations for DAOs.

As for issues related to DAOs in terms of security, an opinion was raised that autonomous initiatives involving participants alone such as bug

bounty are insufficient in the area of security and it is necessary for DAOs to be participated in by a variety of external parties in such ways as certification by third parties, and in this context, DAOs may not be able to be complete by themselves.

As an approach to address the above issues, it may be possible for DAOs to take a form less decentralized and autonomous to solve issues faced by software protocols and smart contracts (and governance and incentive mechanisms, which are the precondition of the foregoing), and then increase the degree of decentralization and autonomy. At this point in time, however, there is no common understanding of what kind of approaches would be effective. Therefore, it is necessary to conduct follow-ups on trends in DAOs.

(v) Discussions on incorporation of DAOs

A. Trends in incorporation of DAOs in various other countries and recognition of issues in Japan

Various countries including the U.K. are engaged in various discussions on laws and regulations which serve as the basis for establishment, management, and operation of DAOs. As for existing DAOs, while there are some whose legal basis is unclear, there are some whose legal basis is on jurisdictions where foundations in a form which goes well with DAOs can be established (e.g.: Cayman Islands and Switzerland) or on jurisdictions where there are systems established bearing DAOs in mind (e.g.: State of Wyoming in the U.S.). When selecting a jurisdiction, various factors affect an organization intending to establish a DAO, such as tax privileges and regulatory supervision by authorities, in addition to the system for DAOs.

In Japan, there is no system under which legal personality is granted to the organizational form per se of DAOs. Many uncertainties have been pointed out, such as the governing law, legal position, details of legal rights and obligations of members and participants, and issues related to tax payment. In this regard, at hearing sessions, it was pointed out that, while legal personality is necessary for an organization to be responsible for its operation, budget management, and other such activities, as there is no system under which legal personality is granted

to DAOs at this point in time, there is a necessity of establishing corporations, separately from DAOs, from the perspectives of rights and interests directed at external parties and fund management.

The document published by the U.K. Law Commission states the following views on DAO-specific incorporations.

- The U.K. Law Commission understands that DAO-specific incorporations may not be attractive to all DAOs for practical, legal, or ideological reasons, especially those that wish to maintain or increase their degree of decentralization.
- However, the U.K. Law Commission also understands that other stakeholders might find a use for these entities: for instance, if they wish to immediately benefit from limited liability; or if they wish to incorporate a limited liability sub-DAO as part of a more complex DAO organizational structure.

In the U.S. State of Wyoming where legislation for DAO-specific incorporations was established ahead of the rest of the world, one of the purposes of incorporation is to eliminate concerns over unlimited liability.

B. Direction of future discussions in Japan

At the Research Group, an opinion was raised that, while benefits of incorporation of DAOs include limitation of liability of members, clarification of matters related to taxation (in the case of the U.S. State of Wyoming, DAOs were subjected to pass-through taxation), and clarification of subjects who will be held liable by third parties and competent supervisory authorities, a more in-depth analysis of needs is needed, as which points to focus on can differ depending on the purpose and type of a DAO.

Among the organizational forms in Japan, the limited liability company form, which is a legal entity with limited liability, which allows for direct democratic decision-making, and whose autonomy through the articles of incorporation is broadly accepted, has been pointed out as a potential foundation for DAOs (if pass-through taxation is not needed). On the other hand, a limited liability company under current law is required to list names and addresses of their members as absolute

matters to be stated in the articles of incorporation. Therefore, incompatibility with DAOs, which are characterized by the anonymity and liquidity of their participants, has also been pointed out if participants of a DAO are to be members of a limited liability company. There are various forms of DAOs, and there could be an argument for using a form other than a limited liability company as the basis for DAOs. However, the Research Group discussed the possibility of, based on the limited liability company form for example, protecting the privacy and anonymity of constituents who are members by listing the identified wallet address of such members instead of their name and address in the articles of incorporation, and streamlining financial reporting and auditing based on on-chain data. Major opinions raised were as described below.

- The desirable approach to take is to clarify what can or cannot be achieved with DAOs under the current systems (for example, limited liability company form) and, if there are systemic issues identified as obstacles, to reexamine the purpose of the system and consider its ideal form.
- It was pointed out that, in cases of other countries which enforced legislation earlier, the legislation does not meet the technical needs (e.g.: management and operation policies and smart contract identifiers related thereto, which are assumed to be determined or updated after establishment of a DAO, is made as a requirement for establishing a DAO). As such, discussion should be based on practical needs.

In addition to the above, there was also a suggestion to consider a new form of organizations which aim to maximize benefits by limiting their time as a form that can only be created with DAOs, not the existing legal form of incorporation.

As stated above (refer to (ii) and (iii)), it is expected that a common understanding of the significance of DAOs in society will be fostered by analyzing various use cases in Japan, which will contribute to the progress in discussions on how DAOs should be incorporated.

(vi) How regulations should be regarding DAOs

Regulations are assumed to be applied according to the actual situation, including the handling of governance tokens issued by DAOs. In this context, the following opinions were raised on how the regulations should be.

- At present, there may be no DAOs that are actually useful to the world. However, DAOs are considered to play an important part in the future of Japan. Therefore, it is important to take an attitude to unlock their potential.
- On the other hand, no legislative bases exist as to why DAOs should be given special treatment. At present, there are no actual cases of DAOs which aim for local revitalization and social contribution. There is a concern that regulations will remain behind forever without the accumulation of actual cases to justify and create exceptions to the regulations.
- It may be good to have a perspective of how to create regulations that are consistent with the three main goals of financial regulations (consumer protection, financial stability, and prevention of financial crime) in the broader world which includes DAOs as well as non-financial aspects.

At hearing sessions held by the Research Group, municipal governments pointed out that they are looking at the Digital Agency to be the cross-ministry help desk to receive inquiries regarding barriers that they have never experienced before come up in the course of administration and community development. The consultation desk established by the Digital Agency needs to conduct ongoing follow-ups in collaboration with related ministries and agencies so that initiatives toward the realization of abovementioned expectations for DAOs are steadily promoted in Japan, while asking municipal governments and others that are promoting DAO initiatives to share their awareness of the issues.

(vii) Expectations for and issues faced by local community DAOs

Local communities have been making moves to use DAOs for issue solution and local revitalization. At hearing sessions held by the Research Group, parties involved in such initiatives pointed out as follows regarding expectations for DAOs.

- As it is becoming increasingly difficult for local communities alone to solve their local issues, it is necessary to use the DAO mechanism and thoroughly open up local communities.
- While we aim to solve local issues, generate new value, and create a new community which uses tokens in a collaborative manner based on ideas given by diverse people gathered at our DAO, we also hope to attract companies which work on Web3.0 in the future.
- We hope to use the power of sympathy and support received from across local communities through our DAO in real local activities, and to link the power to moves such as donations as well as immigration and settlement to the region in the future.
- Diverse human resources who previously had no way to be involved with the local community become able to act for the local community in an inclusively manner through our DAO. This has enabled support for diverse work styles and self-fulfillment.

It is pointed out that local community DAOs have the potential of solving issues and creating value through new forms of human and economic ties. On the other hand, to realize sustainability of such DAOs, there are issues to be considered, such as how the incentive mechanism should be, including governance tokens, and the relationship between real residents and virtual residents (DAO participants).

Regarding how the incentive mechanism should be, at meetings, an opinion was raised that participants in DAOs currently see value in expanding their own activities with the proof of token ownership, not in increasing the secondary distribution price of their token. In response to this, opinions were raised that the following perspectives are required to realize the sustainability of DAOs.

- Local community DAOs are expected to have to bear the expenses such as costs for community management and measures against software vulnerabilities as well as fixed costs. As such, an appropriate incentive mechanism is needed to retain actors who bear such expenses. More specifically, the mechanism should be designed to be sustainable despite volatility, including how to respond to a drop in the secondary distribution price of tokens. Consideration needs to be given to developing an industry so that a give-and-take relationship with participants who purchased

tokens for a fee is created in a sustainable manner.

- Regarding this point, for measures against software vulnerabilities in particular, it is important to take a viewpoint of efficiently leveraging limited human resources by, for example, sharing best practices instead of having individual DAO engineers take measures under diversified silos.

Moreover, the following opinions were raised regarding the relationship between real residents and DAOs.

- In local community DAOs, it is difficult to determine how DAOs should be considered when any discrepancy arises in principles and ideas between real residents and virtual residents (DAO participants). In addition, it is necessary to bear in mind the possibility of conflicts between real residents and virtual citizens over the use of the municipal budget, if such budget is to be used.

As the use of local community DAOs advances in the future, it is expected that knowledge and issues will be accumulated and shared regarding the following matters: what problems can be solved and how local revitalization can be realized through the use of DAOs; what value and significance can be found by DAO participants, both inside and outside the local community, to commit to their activities; what value and incentives will be distributed in what form through governance tokens; how the sustainable relationship with real residents will be built.

(3). Basic direction of sound development of Web3.0

The Research Group discussed issues that should be addressed at present as well as those that should be discussed in the future to realize the ideal future form in which social issues are solved and value is created through new forms of human and economic ties generated by the use of DAOs.

At present, various types of organizations are operated as DAOs, and these moves will possibly increase in the future. It is necessary to first analyze use cases under the current framework, identify benefits and issues more specifically, and consider the ideal form of the system. In so doing, it is necessary that technological issues including security are not discussed within closed circles related to individual DAOs, but rather, measures are considered so that limited human resources are

efficiently used by, for example, sharing best practice. In addition, it is necessary to consider legislative issues such as limited liability for members, including how interests of various stakeholders should be coordinated, from a different perspective than technical issues. It is desirable to first identify the problems under the existing limited liability company form and then consider the direction of action.

In order to promote these and other discussions, it is important that various DAO initiatives be promoted and many use cases be generated in Japan. To this end, the consultation desk established by the Digital Agency needs to conduct ongoing follow-ups in collaboration with related ministries and agencies so that initiatives toward the realization of expectations for DAOs such as solution of social issues and creation of new value are appropriately promoted, while asking municipal governments and others that are promoting DAO initiatives to share their awareness of the issues.

4. Decentralized identity (DID)

Decentralized Identity (DID) realizes a free and competitive environment and service collaboration not relying on platform business operators. On the other hand, it also has issues regarding measures against misconduct and law enforcement. Multilateral collaboration will be necessary to create a safe and reliable environment to use DID and to ensure privacy protection and cross-border interoperability. Web3.0 aims to connect individual elements; which means that ID needs to be established without being dependent on a centralized framework.

(1). DID and discussions thereon

As for digital identity providers, there has been an increasing number of cases where private-sector platform business operators which provide services with excellent operability offer their services and authentication functions to public institutions and other private-sector businesses. This concentration of providers of authentication functions has realized good operability, a high-level of security measures, and data collaboration among organizations. On the other hand, such circumstances may encourage oligopolies by platform business operators, and in addition, damage has been apparent in cases where the providers of such services refuse to provide their services, making many services unavailable in a chain-reaction manner.

In recent years, in light of these risks, initiatives related to DID have been progressing to provide a basis for users to manage and control where their own information is provided without being dependent on specific organizations, contrary to existing digital identity, the issuance and use of which have been centrally managed.

While some have pointed out that a decentralized architecture using blockchain and other technologies is desirable to establish DID, consideration of measures to establish an environment for its practical use based on the developments in technologies and standardization is considered one of the most important issues toward the sound development of Web3.0.

DID/verifiable credentials (VCs)[1] has been discussed as one of the

[1] Verifiable credentials (VCs): Self-sovereign identity certificates which enable online verification of the content, the specifications of which have been proposed by the World Wide Web Consortium (W3C). This is a mechanism in which the validity of a certificate issued by the issuer to the holder can be verified by third parties without requiring them to ask the issuer about the validity.

technologies used in the “Trusted Web”, which aims to add a new framework of trust for the realization of DFFT, such as a mechanism to strengthen the control of data by individuals and corporations without depending on specific services, and a mechanism which enables verification of data transmissions and counterparties thereto. Tests involving use cases and other models are ongoing.

The Research Group held discussions mainly on the following matters. Please refer to [Reference 5] regarding the overview of discussions related to DID.

(2). Main matters discussed by the Research Group and direction of actions

(i) Expectations for potential of DID

There is a possibility that the increasingly common use of DID links services scattered across the public and private sectors without making users dependent on specific platform business operators while avoiding centralized management of information, which may in turn realize a high level of once-only services that are difficult for public institutions to realize.

On the other hand, it also has been pointed out that, while reliable key management functions are required to securely handle DID and digital assets using smartphones, DID may not always allow users to escape the control of platform business operators, because they face issues such as that platform business operators govern hardware-based key management functions which enable secure key management on smartphones.

In addition, there is concern that if DID, which can be used across borders, and for which there is no specific business operator that is responsible for measures against misconduct, is increasingly commonly used, this may impair user protection by business operators, including measures against misconduct, and make law enforcement difficult as a result.

In order to eliminate such concerns, it is considered to be necessary to create an environment in which users can easily obtain wallets which have undergone strict identity verification, and direct users to use secure wallets through concerted efforts among multiple countries.

(ii) Expectations for use of My Number cards and discussions on realization thereof

Based on the application, an electronic certificate for public individual authentication is loaded on a My Number card. An opinion was raised that, even if My Number itself cannot be utilized for the system, private-sector business operators could also conduct identity verification using public individual authentication in DID. In addition, another opinion was raised stating that, as the use of My Number cards increases, it can be expected that the number of citizens with information literacy will increase, and this would stimulate more active discussions and in turn more business operators would implement the system.

As an issue related to the use of My Number cards, the certificates can only be managed by business operators who have been certified by the Prime Minister of Japan and the Minister for Internal Affairs and Communications so that the serial numbers of these certificates will not be abused through such acts as name identification. In addition, when signing a document electronically, the serial number of the certificate will also be included on the signed document. As such, consideration should be given to efforts on devising a way to avoid certificate serial numbers being written on blockchains.

(iii) Discussions on privacy protection

Discussions on the fact that information linked with an identifier can constitute personal information have not been limited to the Research Group. An opinion was raised that, as identifiers and public keys fall under the category of personal information, it may be unacceptable to put them on a public chain and/or make them public, based on the perspective of privacy protection.

On the other hand, while the chain itself is open to the public, various methods can be envisioned for how to selectively disclose only the information one wishes to present, such as a way for one to use different identifiers rather than tying all information to a single identifier, and a way for one, at their own discretion, to tie certain information depending on the circumstances. This is also an area of ongoing R&D. Therefore, it is considered necessary to continue the study while also taking into account the status of R&D.

The use of non-transferable tokens, such as NFTs, non-transferable

tokens (NTTs), and soulbound tokens (SBTs), has been proposed in the case where a public blockchain is to be used as the ledger to manage DID.

All such non-transferable tokens are difficult to complete on-chain from the perspectives of the block size of a chain, economy, privacy protection, and addressing the risk of difficulty in later deletion of data, once such data has been written. As such, it is common to implement the system in such a way that the attribute data substances are placed on a server or in an InterPlanetary File System (IPFS). While proof of existence at a given point in time remains as a record on blockchains, continued operation is necessary to keep it functioning as a service, which means that it is not different from conventional authentication and such other services.

Technologies for privacy protection such as selective disclosure, zero-knowledge proof, and homomorphic encryption have been increasingly used to make DID practical, and parts of these technologies are being applied to the international standards for matters such as loading vaccination certificates, driver's licenses, and general-purpose identification certificates on smartphones. Future in-depth discussions by related parties are expected.

(3). Basic direction of sound development of Web3.0

R&D on DID is underway, and there are a large number of issues that need to be solved before the practical application of DID can occur. More specifically, in the first place, it is difficult to strike a balance between the use of public blockchains and privacy protection, and future R&D is expected.

With the increasing use of digital assets, realization of efficient AML/KYC for on-chain transactions is strongly required (please refer to 6(2)(iii)). As such, it is important to move forward with discussions and examinations toward the practical application of DID in exchanging identity verification information for crypto asset wallets.

There have been international discussions on techniques for exchanging identity verification information of wallet addresses between source exchange service providers and destination exchange service providers. Discussions on how to safely exchange identity verification information which has undergone public individual

authentication, while still protecting privacy, will soon commence using a multi-stakeholder model.

In Europe, there have been steps taken in various countries to issue identification certificates to smartphone app wallets as digital identity wallets. Surveys will be conducted on trends in the creation of the usage environment and international standardization for the realization of secure wallets.

Regardless of whether the commercial application of DID is realized, we will monitor the progress of the related R&D and application of privacy protection technologies, while seeking the advancement of digitalization in Japan and exploring its applicability to the interoperability of services such as identification certificates and reliable data distribution across borders through R&D and contributions to international standardization.

5. Connection with metaverse

The use of the metaverse as a space to realize Web3.0 is being considered in various ways, and there are some cases of services that are oriented to the Web3.0-type metaverse (which combines Web3.0 and the metaverse). While many metaverses that currently exist are “Web2.0-type” (which has an operator and a centralized system), it is possible that Web3.0-type metaverses will be built in the future. Potential scenarios for connecting Web3.0 and the metaverse include cases where avatars and items are exchanged in collaboration between multiple metaverses and where a token economy and NFTs are incorporated in a metaverse (avatars and items are presented in reference to tokens or NFTs recorded on external blockchains). In addition, while, at present, various issues surrounding the metaverse are being examined by the related ministries and agencies, for example, the problems such as the creation of a creator economy, legal position of digital assets, legal issues related to the responsibility of platformers, and methods of solving cross-border disputes among users seem to be points of argument and issues commonly recognized for Web3.0. Based on these points, it is important that the related ministries and agencies work to share information and solve issues in cooperation with one another by taking into consideration the relationships between other issues in Web3.0 (digital assets, DAOs, DID, user protection, and law enforcement) and the metaverse.

(1). Discussions on the metaverse

Attempts to build virtual spaces on computers have resulted in stronger ties with online games, social networking services, and other services. These spaces have recently been called the metaverse. Various services are being offered on the metaverse.

The metaverse, as a new space where technologies and services of Web3.0 are expected to be utilized, can be one element of the sound development of Web3.0. Accordingly, how Web3.0 is connected to the metaverse is one of the important issues to be considered.

Related ministries and agencies are currently examining matters such as how the metaverse could be used.[2]

[2] The Ministry of Economy, Trade and Industry, “Research Project on Creation of Creator Economy in the Era of Web3.0”

Issues related to the metaverse are diverse, as shown in the examples listed below. However, for example, the problems such as the creation of a creator economy, positioning of digital assets, legal responsibilities of platformers, and methods of solving cross-border disputes among users seem to be points of argument and issues commonly recognized for Web3.0.

[Examples of issues related to the metaverse]

Technological issues	・ Improvement of the number of concurrent connections and the number of concurrent users ・ Improvement of interconnection capability ・ Advancement of technologies for the infrastructures as a whole, including the above
Business issues	・ How revenue models are built ・ Creation of creator economy ・ Establishment of systems in which users can safely use the metaverse with peace of mind
Legal issues	・ Protection of intellectual property rights ・ Protection of personal rights ・ Legal position of things purchased in the metaverse, including digital assets ・ Legal liability of platformers ・ Disputes between users may occur across borders.

(Main source: Created by the Digital Agency based on materials from the “Research Group on the Use of the Metaverse Toward the Era of Web3.0,” the Ministry of Internal Affairs and Communications)

It also seems to be important to consider what synergies could be created with technologies and services of Web3.0 and what would hinder to the realization of such synergies, with an eye on changes in distribution of value caused by the metaverse and its ability to promote innovations.

From this point of view, the Research Group held discussions mainly on the following matters.

(since July 5, 2022); the Ministry of Internal Affairs and Communications, “Research Group on the Use of the Metaverse Toward the Era of Web3.0” (since August 1, 2022); and Intellectual Property Strategy Promotion Office of the Cabinet Office, “Public-Private Liaison Committee for Legal Issues Surrounding Content on the Metaverse” (since November 21, 2022)

(2). Main matters discussed by the Research Group and direction of actions

(i) Discussions on the possibilities of the metaverse

The following opinions were presented regarding the potential of the metaverse in the discussions by the Research Group related to the future vision of Web3.0 (refer to 1(3)).

- Through the metaverse, distribution of intangible objects, the value of which is difficult to identify, has become possible. As such, the form and means of distribution of value have been changing. It is expected that, through such developments, communities which have been increasingly divided along with the development of information and communication technologies will once again be connected and create new value.
- Ultimately, there is a possibility that concepts of individuals and free will may change, as seen in cases where an individual person may use multiple avatars or multiple persons share one avatar; under such circumstances, value, ownership, and transactions may be redefined.

In hearing sessions conducted by the Research Group, the following topics were pointed out as the possibilities of the metaverse, which are different from conventional tools.

- Experience in a virtual space as avatars and game characters of the metaverse tends to remain in people's memories for a long period of time as a simulated experience. As such, it would be effective to utilize such experience for education, provision of traveling experience, disaster prevention drills, and other purposes.
- In the metaverse, users use multiple accounts and conduct activities as avatars which have multiple personalities. Therefore, it is possible to collect subdivided movement history. It can also be used as a marketing tool by companies if privacy protection issues can be overcome.

As explained above, the metaverse has the possibility to function as a means of new value creation, or as an alternative means when similar acts are restricted in the real world for various reasons. It is uncertain

what kind of synergies can be produced when this potential and technologies and services of Web3.0 are connected. However, it will be important for the metaverse itself to develop as an industry while having such potential.

(ii) Accounts in the metaverse

Users create accounts on metaverse platforms to engage in activities. Initiatives to allow users to move among multiple metaverses by linking their accounts are considered to be particularly important from the perspective of the connection with Web3.0. In this regard, the following opinions were presented.

- Consideration should be given to protection of personal rights of an avatar identified as oneself.
- Consideration should be given to whether such acts can be balanced with the business model of metaverses which intend to lock in their own users.
- Attention needs to be paid to international developments so that Japan is not isolated from the rest of the world.

While allowing users to move among metaverses is considered to be a matter of interconnection capability, it is necessary to consider how accounts should be designed, in addition to how personal information should be protected and how the terms of use should be stipulated.

(iii) Support for individual creators in the metaverse

In the metaverse, individual creators are important as they can be actors in value creation. The importance of diverse human resources inspiring each other without barriers to promote technological innovations and freely combining publicly available components to make repeated trial-and-error efforts seems to be shared with the global view of Web3.0.

It was pointed out at the Research Group that there is a need for building an environment where individual creators can enter into the metaverse by improving the circumstances in which it is difficult for entities other than companies and other large-scale entities to create a metaverse.

It is important that more diverse actors create value toward the

development of the metaverse, and related ministries and agencies have been moving forward with specific initiatives. In so doing, further discussions on a desirable ecosystem are expected to create a system for promoting further participation by individual creators.

(iv) High rates of birth and mortality in the metaverse industry

As a premise for the connection with Web3.0, it is important that the metaverse develops as an industry. In this regard, it was pointed out at the Research Group that the problem with the “high rates of birth and mortality” situation in the current metaverse industry, in which a large number of small metaverses are created and dissolved, is losses of digital assets held by users due to the dissolution of metaverses. In response, it was also argued that the problem lies in “high rates of birth and mortality” found under the market competition in Japan where exit rates are particularly low.

Further discussions are expected on what impact the situation of high rates of birth and mortality in the metaverse industry could have on not only business operators but also users and individual creators, and whether such situation may be addressed by, for example, improving interconnection capability.

(3). Basic direction of sound development of Web3.0

As a premise for considering how Web3.0 should be connected to the metaverse, an important point is how to establish an environment for the metaverse to develop as an industry in the future. Regarding this point, for example, issues such as the importance of global standards, the possibility of cross-border disputes among users, and how laws should be enforced on such disputes are partially shared by Web3.0. Therefore, it is highly likely that these common problems will materialize concurrently. Based on these points, it is important that related ministries and agencies work to share information and solve issues in cooperation, taking into consideration the relationships between other issues in Web3.0 (digital assets, DAOs, DIDs, user protection, and law enforcement) and the metaverse.

6. User protection and law enforcement

Various problems concerning technologies and services of Web3.0 have occurred globally, and user protection has become an urgent issue. Whatever the technology is, there is no technology that can serve as a “silver bullet” for innovations. It should be fully understood that even new technologies discussed in relation to Web3.0 have risks and issues. In addition, there should also be shared recognition that a large part of these new technologies to be utilized to solve actual issues immediately may still be immature. Fraud, theft, hacking, and other security incidents are also on the rise around the world; however, it has been pointed out that service operators did not accept requests for compensation or refunds for damage in many cases. Discussions on how to protect users are expected to progress around the world in the future, and Japan also needs to take appropriate actions in this regard. In many security incident cases, known attacking methods are repeatedly used. Therefore, an environment needs to be created to share information among stakeholders, including engineers responsible for system construction, and establish a course of action. Improvement of traceability by authorities and crime deterrence effects can be expected by appropriately operating online identity verification (e-KYC). Accordingly, it is necessary to continue paying attention to developments in international discussions held by organizations such as the FATF and conducting follow-ups on and using appropriate methods to ascertain actual circumstances utilizing technologies. In addition, in recent years, the number of inquiries on user problems related to crypto assets has been rapidly increasing. It is important that related ministries and agencies steadily move forward with initiatives such as collection, sharing, and handling of user complaint data, and information provision and awareness-raising to prevent user damage.

(1). User protection and law enforcement and discussions thereon

Various problems concerning technologies and services of Web3.0 have occurred globally, and user protection has become an urgent issue. It is essential for the creation of an environment toward sound development of Web3.0 to study cases that could be a problem from the perspectives of cross-border crimes abusing blockchain technologies and user protection, identify what actions need to be taken

immediately, and consider how user protection and law enforcement should be conducted in Japan at present.

The Research Group held discussions mainly on the following matters, based also on the trends in recent cases. Please refer to [Reference 6] regarding the overview of domestic and international discussions on user protection and law enforcement.

(2). Main matters discussed by the Research Group and direction of actions

(i) Overview of recent cases and discussions on technological actions based on such cases

The bankruptcy of a leading global crypto asset exchange in November 2022 had a knock-on effect and led to multiple bankruptcies. The case presented a wide variety of issues related to governance, asset management, information disclosure, unfair trade, information leakage, money laundering, and security. It is expected that the actual situation of the case will be clarified and discussions will take place based on the findings.

Not limited to this case, crimes related to Web3.0 services have occurred globally and frequently, as described below.

- 2021: According to Chainalysis, the total amount of damage related to crypto assets was about 14 billion dollars (about 1.9 trillion yen), and damage from fraud and theft accounts for 80% of the total damage. More specifically, rug pulls (a method of fraud in which an operator of a project, which is established for fraudulent purposes, collects funds using tokens and other means and swindles the funds) on decentralized finance (DeFi) platforms are said to be rapidly increasing.
- 2022: Until the end of November, according only to public information, it was reported that 37 rug pull cases occurred (the total amount of damage: about 32 billion yen), and the overall security incidents including hacking totaled 105 cases (the total amount of damage: about 402.5 billion yen). Recent incidents included fund outflows from DeFi, theft of digital art NFTs, wash trade in which the prices of NFTs were intentionally raised, money laundering through purchase and sale of NFTs, fund outflows from wallets managed by DAOs, and improper use of funds by founders of DAOs.

Among the above cases, Chainalysis published the following analysis results regarding fraud and theft in particular.

- Fraud: Cases in which operators of DeFi platforms intentionally make the smart contract codes vulnerable and swindle the collected funds have been increasing. In addition, there various techniques are being used, including Ponzi schemes, pyramid schemes, and billing fraud.
- Theft: About 80% of thefts have occurred on DeFi platforms. DeFi has the characteristics of transparent codes, which make hacking easy. Security infringements such as attacks against smart contract vulnerabilities and theft of keys account for the majority of cases. As a technique used to attack smart contract vulnerabilities, there were cases in which prices were manipulated using such methods as oracle attacks, and funds were illegally swindled in flash loans (a system in which tokens are borrowed without collateral on the condition of immediate repayment).

In the meetings of the Research Group, the following opinions were presented, analyzing the above cases.

- The number of security incidents as a whole has been increasing as compared to the previous year. The major reasons for the security vulnerabilities behind this are smart contracts that are increasingly commonly used as well as bridges (a protocol which enables interaction among different blockchains) used to address the issue of scalability arising from the characteristics of blockchain technologies.
- Meanwhile, security incidents currently being observed use known attacking methods, which can be categorized into the following five categories:
  (i) Attacks against old-fashioned crypto asset exchanges
  (ii) Attacks against bridges
  (iii) Attacks against smart contracts
  (iv) Attacks against oracles when taking external data into smart contracts
  (v) Attacks against blockchains through an impact on internet protocols

As an action that can be undertaken from a technological viewpoint based on such analysis, at the Research Group, an opinion was raised that, although these attacking methods themselves are already known and precautions can be taken to a certain degree, the attacks continue because the practice of building blockchains safely is not shared among system designers, and it is important for such practice to be shared among them.

From the perspective of user protection and ensuring reliability, it is important to establish how to handle known attacks and action policies in cases of security incidents. As one of the measures toward this end, it is required to create an environment where stakeholders, including engineers who build systems, conduct fixed-point observation for security incidents, verify their relevance with the development of technologies, and share information on a regular basis. (→[Please refer to 2. Digital Assets (2)(v) Discussions on security.])

On the other hand, from the perspective of user protection, cases have been observed in which operators of services including DeFi share information on SNSs or using such other means; however, no common framework that ensures the truthfulness of information or serves as the basis for compensation for victims has been identified. In addition, it was also pointed out that, in many cases, service operators held customers responsible for management of their own accounts and did not accept requests for compensation or refund for damages. In the future, discussions on how users should be protected are expected to progress on a global scale by taking into consideration various issues identified in the bankruptcy of a leading global crypto asset exchange in November 2022. Accordingly, appropriate actions need to be taken in Japan as well, based on global developments.

(ii) Discussions on importance of online identity verification (e-KYC)

According to a report from the U.S. Department of Justice,[3] funds are actively transferred using the anonymity of crypto asset transactions, and matters such as the following are pointed out.

- It has been difficult to conduct identity verification in transactions

[3] "How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets" (published in June 2022)

using unhosted wallets (wallets managed by individuals) for which know your customer (KYC) procedures have not been conducted.

- Techniques are observed in which identification of how funds are distributed is made difficult by, for example, making transactions complex and anonymous. More specifically, techniques such as the following are used: (1) DeFi transactions which are made more complex by using cross-chain technologies; (2) use of tokens which can anonymize transaction records; and (3) decentralization and anonymization of transaction records using mixing services.

In keeping with the developments in regulatory compliance using technologies (RegTech for regulatory compliance by business operators and SupTech for actions by regulatory authorities), private-sector business operators have been observed to be providing business operators and regulatory authorities with services such as online know your customer (e-KYC) procedures, tracing and analysis of transaction records, risk assessment of wallet addresses, and transaction monitoring. Specific services include the following:

- e-KYC, certification services at the time of transactions using collected identity information, and accumulation and provision of information on accounts which are sharing facial and other attributed information or conducting other improper acts;
- Tracing of transaction records of crypto assets and investigation of entities and fund routes which are behind the addresses being investigated;
- Making crypto asset transactions visible (such as by analyzing linkage between wallet addresses) and monitoring of the status of deposits and withdrawals;
- Risk assessment for crypto asset service providers, including crypto asset exchanges; and
- Risk assessment of addresses which are counterparties in transactions (wallet screening).

In the meetings of the Research Group, it was pointed out that it is extremely important to operate e-KYC appropriately because tracing will become very difficult if identities are not verified appropriately; therefore, increasing the effectiveness of identity verification will

increase traceability, and at the same time, may prevent crimes.
In addition, at the hearing sessions conducted with business operators who provide the RegTech/SupTech services mentioned above, it was pointed out that, while currently, unhosted wallets and other similar means used by crypto asset exchanges and other service providers can be used without identity verification, in the future, systems may be introduced in which individuals hold identity verification information and present the identity information to authorities when necessary.

As stated in 4(3), realization of efficient AML/KYC in on-chain transactions has also been an important perspective in the discussion of the practical application of DID. Related ministries and agencies continue to be required to conduct follow-ups on and use appropriate methods to ascertain actual circumstances utilizing technologies.

(iii) Discussions related to actions to be taken for inquiries from users

In regard to the status of acceptance of inquiries related to crypto assets from users, according to the National Consumer Affairs Center of Japan:

- The number of consumer affairs inquiries regarding crypto assets registered in the PIO-NET (nationwide consumer affairs information network system) was 5,466 (in 2021), and one third of the inquiries were from contracting parties who are in their 20s and 30s. In the U.S. as well, the number of inquiries rapidly increased over the period from 2021 to 2022.
- In such inquiries, problems seem to be triggered by solicitation from persons the inquirer met on SNSs and dating apps, or from their acquaintances and friends.

In regard to the status of acceptance of inquiries related to NFTs from users, according to the National Consumer Affairs Center of Japan:

- The number of consumer affairs inquiries regarding NFTs registered on the PIO-NET was 4 in FY2021, and 4 in FY2022 (cases registered on the system by June 15).
- The details presented by the Center included a case in which an inquirer was deceived by an operator who explained that the inquirer would receive a considerable payment if the inquirer

became the owner of an NFT game character and received payment from the inquirer; a case in which an inquirer sent their crypto assets to purchase a digital artwork with an NFT of celebrities, but it was a fake website; and a case in which an inquirer sent their artwork to a person who sells drawings as NFT art but received no consideration for that.

The U.S. Executive Office of the President announced (in September 2022) measures focused on handling and utilizing consumer complaints as listed below.

i. Active promotion of investigations and enforcement actions against illegal acts in the area of digital assets (Securities and Exchange Commission/Commodity Futures Trading Commission)
ii. Doubling initiatives toward enforcement against unfair, fraudulent, or illegal acts based on consumer complaints monitored (Consumer Financial Protection Bureau/Federal Trade Commission)
iii. Formulation of guidance and other such documents related to risk treatment for the digital asset ecosystem
iv. Sharing of consumer complaints data among relevant organizations
v. Awareness-raising activities for consumers on the risks of digital assets and fraudulent acts (Financial Literacy and Education Commission)

Japan also needs to consider what systems should be established that are effective from the perspective of user protection, in reference to these measures. It is important that related ministries and agencies steadily move forward with initiatives such as collection, sharing, and handling of data related to inquiries accepted from users, enhancement of precision of analysis, and information provision and awareness-raising to prevent user damage. Whatever the technology is, there is no technology that can serve as a “silver bullet” for innovations. More specifically, it should be fully understood that even new technologies discussed in relation to Web3.0 have risks and issues. In addition, there should also be shared recognition that a large part of these new

technologies may still be too immature to be utilized for solving actual issues immediately.

●Number of consumer affairs inquiries related to crypto assets in Japan

Figure 1 Number of inquiry cases by fiscal year

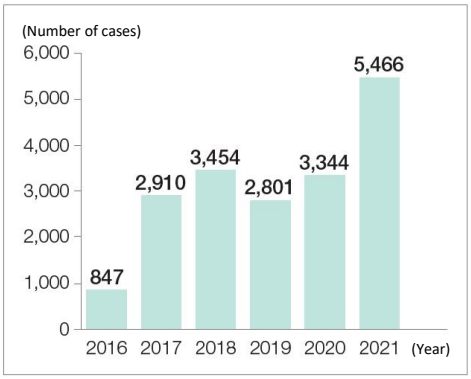
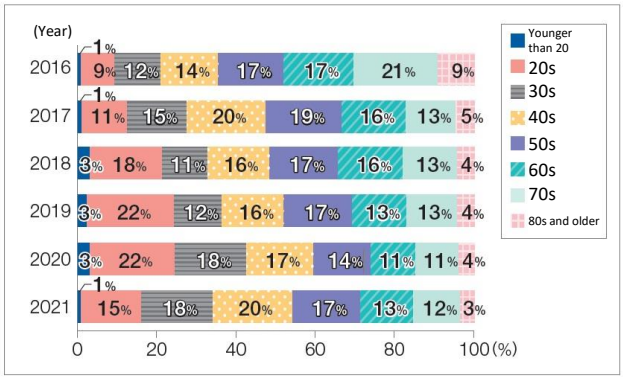


Figure 2 Ratio of inquiries by age range by fiscal year

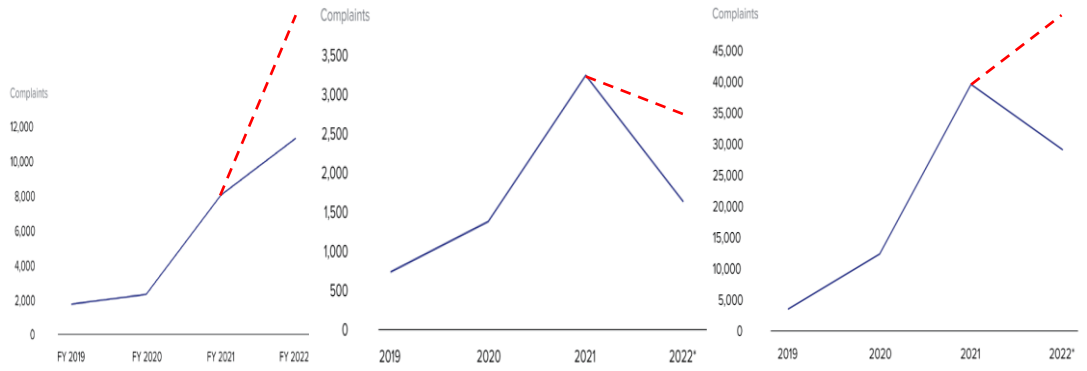


＊1 Practical Living Information Online Network System (PIO-NET) is a database that accumulates information on inquiries related to consumer affairs through an online network of the National Consumer Affairs Center of Japan, consumer centers across Japan, and other such organizations. The data does not include inquiries made via consumer centers and other such organizations. The data referred to in this report is that registered with PIO-NET by February 28, 2022.

＊2 The data was compiled from inquiries related to "crypto assets" (including "virtual currencies," "cryptocurrencies," and "value records") and does not include inquiries related to in-game currencies (e-money) used for such purposes as purchasing items in online games. Revisions were made in FY2021. Therefore, chronological comparisons cannot be made for FY2020 and before, and after FY2021.

(Source) "National Consumer Affairs" (web version) NO. 117 (May 2022) (National Consumer Affairs Center of Japan)
https://www.kokusen.go.jp/pdf_dl/wko/wko-202205.pdf

●Number of inquiries related to crypto assets in the U.S. (accepted by SEC, CFPB, and FTC, from left)



(Source) The U.S. Financial Stability Oversight Council (FSOC), "Report on Digital Asset Financial Stability Risks and Regulation" (published on October 3, 2022). The figures for 2022 are limited to those accepted up to July 31. The red dotted lines indicate the numbers that are obtained by the Digital Agency, which divided such data by 7 and multiplied the result by 12 for reference purposes. The number of cases accepted by the Securities and Exchange Commission (SEC) since 2019 is over 23,000. The numbers accepted by the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) may be redundant with other authorities.

(iv) Discussions on measures against cross-border crimes

The Web3.0 world, in which many activities occur across borders, is

prone to various cross-border crimes as well. For cross-border crimes, the tracing of suspects becomes difficult due in part to complex and anonymous transactions. Under such circumstances, collaborative actions by investigative agencies of various countries have become more active to combat abuse of blockchain technologies, take down dark web criminal forums, and prosecute hackers who use certain viruses.

Regarding measures against cross-border crime, the following issues have been pointed out in the U.S., in addition to the difficulty in tracing due in part to anonymization.

- The location of the crime organization (such as a business operator and substantial service provider) is unknown, so it is difficult to identify which country to ask for cooperation in an investigation.
- There is a possibility that the country in which the crime organization is undertaking its activities does not cooperate.
- There is a possibility that collecting necessary information is difficult, even if such country cooperates, due to the laws and regulations of each country.

Under the recognition of such issues, in addition to international investigative collaboration, the U.S. has been undertaking initiatives such as the creation of specialized teams (e.g., the Department of Justice established a cryptocurrency enforcement team (in February 2022), and the Federal Bureau of Investigation (FBI) established a crypto asset unit (in March 2022)), participation in and information provision at international meetings, and sharing of expertise with various countries.

For cyber incidents, the National Police Agency of Japan also established the cyber police bureau and the special cyber investigative unit in April 2022, which strengthened collaboration with foreign investigative agencies and other such organizations.

It is essential that various countries undertake measures against cross-border crime, including system establishment, international investigative collaboration, and information sharing. Japan also needs

to work on strengthening systems of relevant organizations and collaboration with foreign investigative and other agencies to counter cross-border crime.

(3). Basic direction of sound development of Web3.0

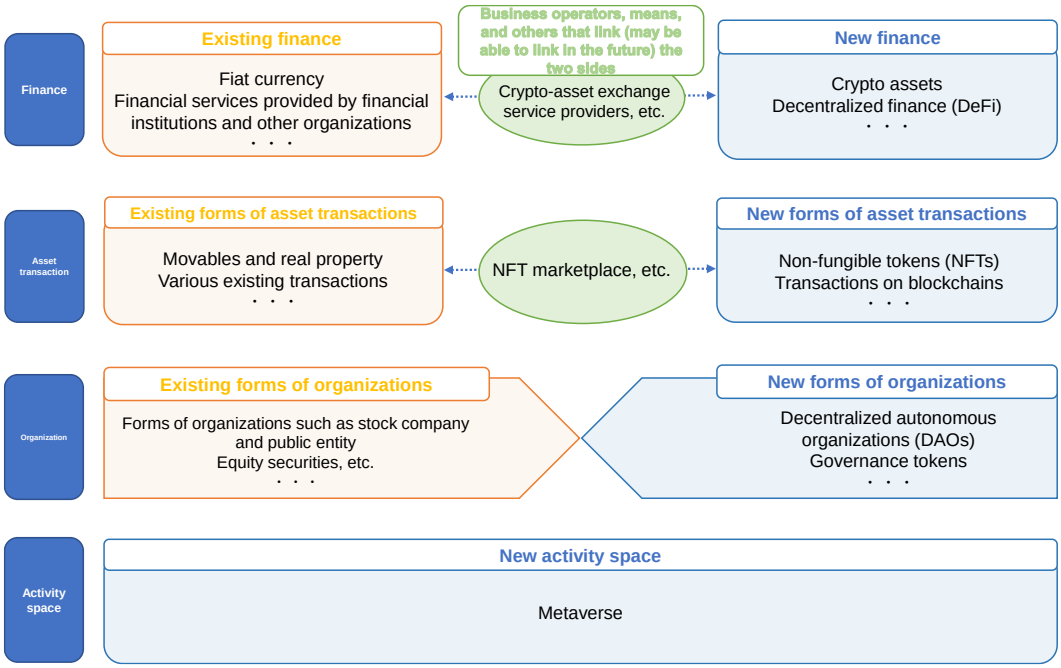
Among the points regarding user protection and law enforcement, the Research Group held discussions mainly on the points in regard to what actions need to be taken against cross-border crime in particular.

In order to realize user protection and build trust for the sound development of Web3.0, it is necessary to establish systems within Japan and continue strengthening international collaboration so that appropriate actions can be taken against cross-border crime. In addition, ascertaining, analyzing, and utilizing inquiries from users are also important issues. Therefore, it is crucial that related ministries and agencies steadily move forward with initiatives such as information provision and awareness-raising to prevent user damage in collaboration with each other.

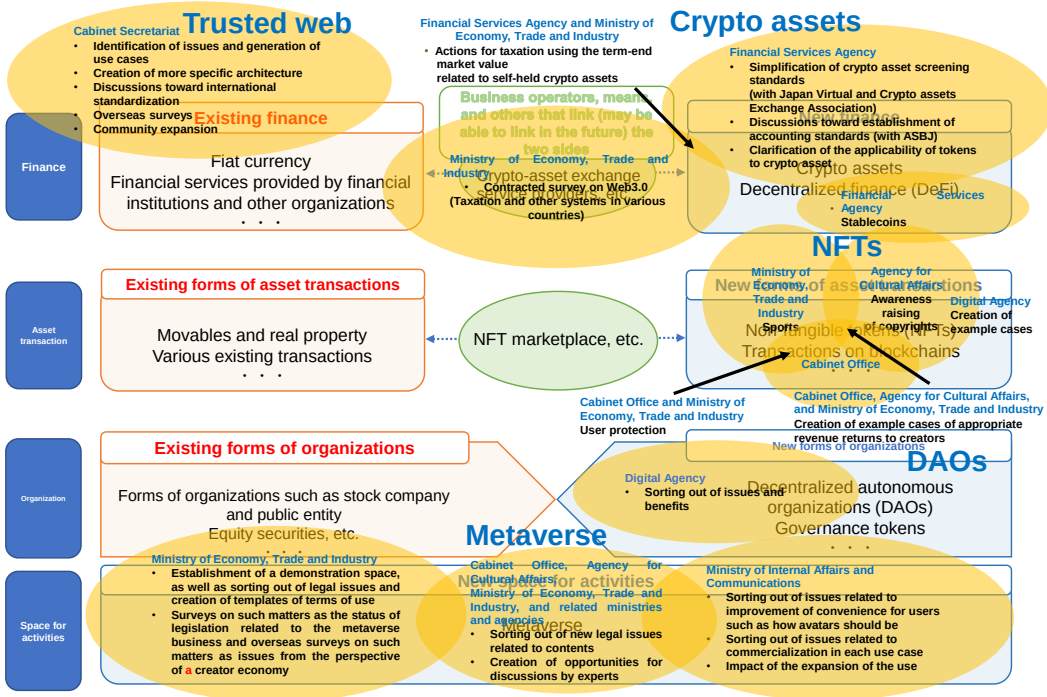
Reference Materials

[Reference 1] Initiatives by related ministries and agencies

A) New technologies called Web3.0 and its future vision (hypothesis)



B) Initiatives by related ministries and agencies mapped on A)



C) Specific initiatives

Area		Description	Timeframe	Ministries and agencies, etc., in charge
Web3.0 in general	Survey	Contracted survey related to Web3.0	Until Dec. 2022	Digital Agency
Crypto assets, etc.	Survey	Contracted survey related to Web3.0 (Survey on taxation and other systems in various countries)	Until Mar. 2023	Ministry of Economy, Trade and Industry
Crypto assets	Screening standards	On November 14, 2022, the Japan Virtual and Crypto assets Exchange Association submitted proposed amendments to self-regulatory rules regarding simplification of crypto asset screening for public comments.	Until Mar. 2023	Financial Services Agency
Crypto assets	Accounting	With respect to the accounting treatment of self-issued and self-held crypto assets, ASBJ announced its view that such assets are not evaluated at fair value until a transaction with a third party occurs. (Accounting standards for crypto assets are to be established after points of argument are sorted out and made public to solicit opinions.)	From Mar. 2022	Financial Services Agency
Crypto assets	Audit	It is planned that an environment in which audits can be conducted by certified public accountants and auditing firms will be created in collaboration and cooperation with private-sector industry associations to facilitate audit of token businesses.	From Dec. 2022	Financial Services Agency Ministry of Economy, Trade and Industry
Crypto assets	Taxation system	Submission of requests for tax reforms including exclusion of self-issued and self-held crypto assets from taxation using the term-end market value[4]	FY2023 tax reform	Financial Services Agency Ministry of Economy, Trade and Industry

[4] 2023 Tax Reform Outline includes the following statements.
"The following revisions will be made to such matters as how crypto assets are evaluated:
(i) Crypto assets that meet the following requirements shall be excluded from the scope of crypto assets held by a

Tokens	Interpretation	On December 16, 2022, proposed amendments to administrative guidelines were submitted for public comments to clarify the applicability of items, content, and other things issued on blockchains to crypto assets	Until Mar. 2023	Financial Services Agency
Tokens	Interpretation	Clarification that businesses handling security and other tokens are subjects of investment by investment limited partnership (LPS)	Until Mar. 2023	Ministry of Economy, Trade and Industry
NFTs	Sorting out of issues	Sorting out and announcement of issues related to the use of NFTs in the sports industry	Announced in Dec. 2022	Ministry of Economy, Trade and Industry
NFTs	Creation of example cases	・ Shared the usage experience through an initiative of delivering certificate of commendation for “JAPAN DIGITAL DAYS” in the form of NFT ・ Considered experimental issuance of occupational history certificates of employees in the form of NFT	・ From Oct. 2022 to Jan. 2023 ・ TBD	Digital Agency
NFTs	Creation of example cases	Creation of example cases of receipt of royalties that are appropriate revenue returns to content creators	From Nov. 2022 for the Agency for Cultural Affairs	Cabinet Office Agency for Cultural Affairs Ministry of Economy, Trade and Industry
NFTs	Right holder protection	Dissemination and awareness raising activities regarding rights infringement including a relationship between NFTs and copyrights	From Jan. 2022	Agency for Cultural Affairs
NFTs	User protection	Collaboration with private-sector initiatives to address user protection issues such as sale of unlicensed NFTs	From Aug. 2022 to Mar. 2023	Cabinet Office Ministry of Economy, Trade and Industry

corporation at the end of a fiscal year for which valuation gains or losses are recognized based on valuation at market value:
A. Crypto assets issued and held continuously by itself since the issuance
B. Crypto assets whose transfer has been continuously restricted from the time of the issuance by any of the following methods:
(a) technical measures being taken to make transfer to other parties impossible;
(b) crypto assets being made as trust assets held in a trust that meet certain requirements;
(The rest of the text omitted.)”

DAOs	Sorting out of issues related to benefits	Planning to share usage experience of the Web3.0 Research Group DAO	From Nov. 2022	Web3.0 Research Group and others
NFT and the metaverse	Sorting out of issues	Responding to new legal and other issues surrounding content and others in the metaverse (such as protection of the rights of virtual objects, avatars, and other matters, and infringement of the rights of others by them) ・ Creation of opportunities for discussions by experts and others to understand issues and sort out points of argument ・ Related ministries and agencies and private-sector business operators make unified efforts to establish necessary rules, including measures based on soft laws.	From fall of 2022	Cabinet Office Agency for Cultural Affairs Ministry of Economy, Trade and Industry
Metaverse	Survey	Overseas surveys on matters such as human resources in short supply in Japan and issues in entry into overseas markets are conducted from the perspective of a creator economy in the Web3.0 era, including surveys on the status of legislation related to the metaverse business and monetization case studies.	From July 2022 to Mar. 2023	Ministry of Economy, Trade and Industry
Metaverse	Sorting out of issues	(i) Issues related to improvement of convenience for users, including how avatars should be in the metaverse; (ii) sorting out of issues related to commercialization in each use case; and (iii) sorting out of impact that the expansion of the use of the metaverse and other technologies has.	From Aug. 2022 to around summer of 2023	Ministry of Internal Affairs and Communications
Metaverse	Sorting out of issues	Establish a demonstration space of the metaverse to sort out legal issues and create templates of terms of use,	From July 2022 to Mar. 2023	Ministry of Economy, Trade and Industry

		aiming for realization of the interoperability of avatars and XR objects		
Trusted web	Survey	Overseas surveys (the status of initiatives related to trusted web, such as identity and verifiable credentials)	From Aug. 2022 Mar. 2023	Cabinet Secretariat Digital Agency
Trusted web	Sorting out and formulation of policies	A white paper summarizing the concept and other matters of the trusted web which aims to rebuild trust in the new digital society, was formulated in 2021 taking into account such factors as concerns over privacy and data reliability. Subsequently, the discussions were continued and the white paper was updated as white paper ver. 2.0 on August 2022 by adding the architecture and other aspects. The white paper will be further improved in the future toward the realization of trusted web.	From Mar. 2021	Cabinet Secretariat Digital Agency
Trusted web	Sorting out of issues	Use cases were solicited from private-sector companies for which development support will be provided, and the selection process has been completed. Going forward, issues toward the realization of trusted web will be identified while making issues that can be solved visibly, and the above white paper will be updated.	From Jul. 2022	Cabinet Secretariat Digital Agency
Trusted web	Overseas collaboration Standardization	Collaboration with overseas related organizations and discussions toward international standardization (holding of sub-working groups starting from around October 2022)	From 2021	Cabinet Secretariat Digital Agency
Trusted web	Community expansion	Aim to expand the base of the community (engineers and business-related and other parties) by launching a website	From 2022	Cabinet Secretariat Digital Agency

[Reference 2] Major policy issues related to tokens and points of argument regarding associated rights

●Major policy issues related to tokens

	Point of argument	Issue
Entity	Startups	Taxation systems, accounting rules, and regulatory reforms
	Revitalization towns and regions	Lack of human resources, public accounting, rules for issuance of bonds, etc.
Subject	Settlement and payment methods	Ensuring provision of utility token services Stability of stablecoins and assessment of backing and other assets
	Means for fund-raising	Information disclosure, insider trading, and market manipulation
	Works, use rights, etc.	Clarification of rights represented, measures against piracy, and creator protection
	Metaverse, game items, etc.	Clarification of rights represented and international standardization
	Membership rights	Investor protection
	Real property	Investor protection and user protection
Transaction	AML/CFT	Identity verification and on-chain cross-border transactions
	Disclosure and insider regulations	Information disclosure, insider trading, and market manipulation
	Measures for users, enforcement of laws	Monitoring of user damage and international collaboration and cooperation among relevant organizations and other bodies
	International collaboration	Collection of information toward and active contribution to establishment of international rules
Record	Treatment under the Civil Code and perfection against third parties	Treatment under the Civil Code and requirements for perfection against third parties
	Ledgers concerning organizations, entities, etc.	Registration of decentralized autonomous organizations (DAOs) as corporations
	International standardization and development of standards	Development of cryptographic algorithms, anonymization technology, data standards, etc.

●Issues and points of argument under the categories based on rights associated with tokens

	Issue and point of argument	Risk and point of argument
Purpose	Settlement and payment	Tokens used as a payment method are categorized as crypto assets
	Fund-raising	If tokens are used as a means for fund-raising, consideration may need to be paid to such factors as accounting standards,

		information disclosure, insider trading, market manipulation
Design	General acceptability	Categorization focused on the circumstances of distribution, not the technological method, is necessary.
	Beneficial interest	Tokens with beneficial interest have the applicability to securities
	Voting rights	Monitoring of such matters as the holding ratio and substantial controllers is necessary.
	Use rights	For utility tokens that can be used for certain goods and services, how the provision of such services should be secured? Are these tokens qualified as prepayment method?
	Anonymity	Useful for privacy protection, but may be abused for money laundering and similar acts
	Transferability	Can be used as decentralized IDs, if tokens cannot be traded on markets due to transfer restrictions
	Price stability	Information disclosure and audit for underlying assets are necessary if the value is based on backing assets For mechanisms of stabilization of assets other than underlying assets through algorithms, close examinations on preconditions and risk scenarios that are functioning are necessary.
	Total volume to be issued	Consideration needs to be paid to such matters as dilution of risks if the total volume to be issued is variable
Infrastructure	Agreed algorithm	Electricity consumption in Proof of Work (PoW) Applicability to securities in Proof of Stake (PoS)
	Cryptographic algorithm	Safety of new algorithms not listed in CRYPTREC and other projects
	Chain layer	How the safety of new chains, L2, and other such chains should be confirmed

[Reference 3] Overview of discussions on digital assets[5]

A) International comparison of financial legislation related to crypto assets and security tokens
B) Tokens that are not qualified as crypto assets and security tokens
C) Delivery of NFTs as certificate of commendation for "JAPAN DIGITAL DAYS"
D) Initiatives such as trial issuance of NFTs to certify employees' work experience
E) International comparison of accounting standards and tax treatment for tokens
F) Rights and interests and legal issues concerning various tokens including NFTs

A) International comparison of financial legislation related to crypto assets and security tokens

- In Japan, the amended Payment Services Act was enforced in 2017. Systems for crypto assets (then virtual currencies in 2017) were established under this Act under which registration as a Crypto-Asset Exchange Service (then Virtual-currency Exchange Service in 2017) is required to conduct a service for exchanging crypto assets and fiat currencies in Japan. The amended Payment Services Act enforced in 2020 requires Crypto-Asset Exchange Service providers to manage crypto assets of their customers using a highly safe method (such as cold wallet). In addition, it was clarified that acts of issuing tokens with rights to receive revenue is subject to the Financial Instruments and Exchange Act. The amended Financial Instruments and Exchange Act enforced in the same year established, among other things, obligations to disclose information to investors and regulations on sale and solicitation for parties including token trading intermediary service providers. Moreover, a system was established as part of AML/CFT to require Crypto-asset Exchange Service providers and other such business operators to conduct identity verification, along with other measures, when opening accounts for customers. On the other hand, there are no AML/CFT and other regulations for tokens which are not qualified as crypto assets and other such assets.
- While it is understood that there are no regulations specific to crypto assets under the U.S. Securities Act, if the use of general digital assets meets the requirements of Howey Test ((i) an investment of money, (ii) in a common enterprise, (iii) with the rational expectation of profit, and (iv) to be derived from the efforts of others), then it is qualified as an investment contract, and registration with the U.S. Securities and Exchange Commission (SEC) is required for the use[6] under the Securities Act, unless registration exemption

[5] The secretariat to the Digital Agency created [Reference 3] through [Reference 6] based on insights obtained from the "Survey and research on the use of digital assets and distributed ledger technology and the development of business environment in Japan," which was conducted by Deloitte Tohmatsu Consulting LLC based on entrustment by the Digital Agency. Interim and final reports of this survey and research are published on the website of the Digital Agency.
[6] The SEC has announced a framework for determining whether digital assets meet the Howey Test requirements.

requirements are met. In fact, there are cases of prosecution on the ground of violation of the same act[7]. In addition, the draft amendments to the rules announced by the SEC in March 2022 proposed to include communication protocols and others as exchanges subject to regulation. As such, decentralized crypto asset exchanges and platforms that use market-making protocols may become subject to regulation. Moreover, crypto assets are understood as being qualified as commodities under the Commodity Exchange Act, and are subject to regulations and other rules on unfair transactions of commodity derivatives and in-kind commodities under the same act. In fact, there are cases of prosecution on the ground of violation of the same act[8]. Furthermore, under the Bank Secrecy Act, which governs the regulations for AML/CFT, obligations such as registration with the Financial Crimes Enforcement Network (FinCEN), identity verification of customers, and detection of suspicious transactions are imposed if engaging in services including transfer of currencies or other value equivalent thereto.

- In Germany and France, under the current laws, assets equivalent to digital assets are positioned as “financial instrument” and “digital asset.” Obtaining of a license which is required under the existing financial legislation when engaging in services subject to the license is obligated, and AML/CFT regulation is applied, accordingly. The draft MiCA regulation currently being discussed by the European Parliament proposes regulations to ensure appropriate functioning of the crypto asset markets while also ensuring the protection of customers by crypto asset[9] holders and crypto asset service providers. In the U.K., Crypto-asset Exchange Service providers and custody wallet providers are required to take measures such as registration with the Financial Conduct Authority (FCA) based on the rules concerning AML/CFT.

B) Tokens that are not qualified as crypto assets and security tokens

- NFTs are believed to be not qualified as crypto assets and security tokens, in principle. There is no unified definition of NFT. However, generally speaking, it is a unique digital

[7] On July 25, 2017, the SEC published a report, in which the SEC pointed out that tokens sold by the DAO in the past were securities in reference to the Howey Test requirements, and therefore, the DAOs should have taken predetermined procedures such as registration of securities, because the past ICO corresponds to the sale of securities.

[8] On September 22, 2022, the Commodity Futures Trading Commission (CFTC) imposed a fine of 250,000 dollars on bZeroX and its two founders on the grounds that they provided leverage transaction services for crypto assets in a manner not compliant with the Bank Secrecy Act and the Commodity Exchange Act. In addition, the CFTC filed a suit against Ooki DAO, which was deemed to have substantially succeeded the business of bZeroX, as an unincorporated association, with the District Court of California. Ooki DAO’s governance token OOKI was listed on Coinbase in August 2022, and said to have 3.9 million holders

[9] Crypto asset: a digital representation of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology (categorized into the following three sub-categories): (i) e-money token: a type of crypto asset that purports to maintain a stable value by referencing to the value of one fiat currency; (ii) asset-referenced token: a type of crypto asset that is not an e-money token and that purports to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more fiat currencies; and (iii) a utility token and other similar tokens: a type of crypto asset which is only intended to provide access to goods or a service supplied by the issuer of that token.

token identifier[10] recorded in a blockchain that cannot be easily forged or falsified. They may have such functions as transaction history tracing and allocation of fees for resale to original authors. The nature varies[11] and how it is positioned in laws, regulations, and other rules needs to be determined specifically on a case-by-case basis[12].

- The FATF, an international cooperative framework for anti-money laundering and other issues, is promoting discussions on how AML/CFT regulation on NFTs should be. The crypto asset guidelines revised in October 2021[13] states that NFTs, which are unique and in fact used as collectibles, not as a means for payment or investment, are not basically crypto assets in light of the purposes of the FATF's standards; on the other hand, it is necessary to apply the FATF standards to NFTs if, for example, NFTs have the same functions as crypto assets (used for payment or investment[14]). "TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS[15]" announced in June 2022 states that, while there are reports suggesting that criminal offenders may abuse NFTs for money laundering and market manipulation, the fact that definitions and functions of NFTs vary in various countries and regions, and this may be an issue in determining how the AML/CFT regulation should be actually applied.
- In September 2022, the U.S. Government announced its policies to assess illicit finance risks related to NFTs and to examine whether regulation on illicit finance shall be applied to digital asset service providers including digital asset exchanges and NFT platforms[16].
- In Japan, the necessity to clarify the interpretation on NFTs' applicability to crypto assets has been pointed out, because, if there are a large number of similar NFTs, they may be used as a method for payment and other such purposes. In response, the Financial Services Agency plans to clarify applicability of tokens including NFTs to crypto assets focusing on whether they have functions as a payment method.

---

[10]The MiCA regulation (draft in Nov. 2022) states that "This Regulation should not apply to crypto assets that are unique and not fungible with other crypto assets, including digital art and collectibles, whose value is attributable to each crypto asset's unique characteristics and the utility it gives to the token holder." It also states that "The sole attribution of a unique identifier to a crypto asset is not sufficient to classify it as unique or not fungible. The assets or rights represented should also be unique and not fungible for the crypto asset to be considered unique and not fungible."

[11] The FATF's survey report in June 2022 states that NFTs have various forms and applications ranging from artworks to representation of ownership of physical assets; for example, assets (property) may be sold using NFTs, and NFTs can be used as collateral for borrowing and lending virtual assets.

[12] For example, in Japan, "coins" are prescribed by the Act on Currency Units and Issuance of Coins, and can be used as fiat currency. NFTs are not qualified as coins. NFTs themselves are digital data, and therefore, are not "tangible objects" which are subject of ownership under the Civil Code. It is necessary to examine whether NFTs themselves can be considered as "rights" based on legal and other grounds.

[13] Revised the "Guidance for Risk-based Approach to Crypto Assets and Crypto-asset Exchange Service Providers" on October 28, 2021.

[14] Attention needs to be paid to the fact that crypto assets under Japan's Payment Services Act refer to those with functions as a means of payment, and their definition is different from that of crypto assets (virtual assets) in discussions by the FATF.

[15] TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

[16] Report on the six key priorities identified in the "Executive Order on Ensuring Responsible Development of Digital Assets" (March 2022) (announced on September 16, 2022)

- It is argued that the U.S. regulations on NFT platforms are not clear and it should be clarified in which cases NFTs are qualified as investment contract and regulated under the Securities Act[17]. More specifically, it was pointed out that NFTs that include governance rights, NFTs that offer investors rights to revenue streams, and fractional NFTs (NFTs newly originated through split of NFTs) could be regulated under the Securities Act[18]. In addition, law enforcement cases concerning NFTs include: (i) a case in which a cease-and-desist order was issued alleging that the sale of online casino NFTs through which sharing of profits was promised is considered as sale of unregistered securities[19], and (ii) a case in which an employee of an NFT platform was prosecuted for such crimes as wire fraud, on the ground that the employee made personal gain through insider trading related to NFTs before the disclosure thereof[20].
- The draft MiCA regulation in Europe states that this regulation should not apply to crypto assets that are unique and not fungible with other crypto assets, including digital art and collectibles. It also states that the value of such crypto assets is attributable to each crypto asset's unique characteristics and the utility it gives to the token holder[21]. On the other hand, it states a view that fractional NFTs would be regulated and therefore attention should be paid to the applicability to NFTs[22]. It also requests that European Securities and Markets Authority (ESMA) publish guidelines to clarify how to distinguish crypto assets which are subject to the regulation and financial instruments which are not.

C) Delivery of NFTs as certificate of commendation for "JAPAN DIGITAL DAYS"

- As a test, the Digital Agency issued certificates of commendation of "good digital award" for digital JAPAN DIGITAL DAYS (October 2 and 3, 2022) in not only a paper format but also a digital format.
- In issuing such certificates, the Digital Agency sought to meet the following requirements.
  - ➢ It can be verified that they are certificates issued by the Digital Agency.

[17] FT 2022/10/17: SEC must clarify which NFTs will be regulated, says commissioner https://www.ft.com/content/e8df6ea4-e9fb-4058-9a36-cef9c12f4726
[18] FT 2022/10/17: SEC must clarify which NFTs will be regulated, says commissioner https://www.ft.com/content/e8df6ea4-e9fb-4058-9a36-cef9c12f4726
[19] Chris Prentice "State Securities Regulators Order Virtual Casino Firm to Stop Selling NFTs" (Thomson Reuters) April 13, 2022
[20] On June 1, 2022, the Department of Justice and FBI prosecuted a former employee of OpenSea for such crimes as wire fraud related to NFT transactions based on insider information. The employee was charged as he allegedly made a personal monetary gain by conducting NFT transactions based on insider information which was planned to be disclosed on the company's website. For this case, on August 19, 2022, a petition was filed asking judges to throw out the case, based on the allegation that prosecutors were stretching the law to "plant a flag in the blockchain industry."
[21] Similarly, the regulation also does not apply to crypto assets representing services or physical assets that are unique and not fungible, such as product guarantees or real estate. The draft MiCA regulation states that, while these crypto assets might be traded in market places and be accumulated speculatively, they are not readily interchangeable and the relative value of one crypto asset in relation to another cannot be ascertained by means of comparison to an existing market or equivalent asset. It also states that such features limit the extent to which these crypto assets can have a financial use, thus limiting risks to users and the system, and justifying the exemption from the application of the regulation.
[22] The draft MiCA states that "The fractional parts of a unique and non-fungible crypto-asset should not be considered unique and not fungible." https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf p10

- The certificates can be reviewed through the wallet of the award recipients as they have been issued as NFTs.
- The Digital Agency uses decentralized technologies to the extent possible.
- The Digital Agency adopts open technologies in line with the global standards.

・ As a result of examination of specifications that meet the above requirements, the Digital Agency decided to combine the two technologies: verifiable credentials (VCs) and non-transferable NFT. An open source tool called Blockcerts was selected as a mechanism to issue VCs.

・ In addition, the certificates were made available for review at any time through the wallet of award recipients by issuing non-transferable NFTs with a link to the aforementioned certificate to the award recipients, through the Ethereum network.

・ (Certificates of commendation will actually be issued to the wallet of the award recipients in January 2023.)

・ Through the test, it is possible to issue digital certificates of commendation on blockchains which can be verified by third parties; however, the following issues regarding the permanence remain.

- Permanence of ID files of the issuer: In this test, the decentralized ID (DID files) needed to verify the issuer was placed on the website of JAPAN DIGITAL DAYS. This website has become a single point of failure, and if this website is erased, the validity will not be able to be verified.
- Permanence of the IPFS gateway: The IPFS has been used as a place to store NFTs and VCs. If the nodes are not managed appropriately, the files themselves may become impossible to access. This time, the Digital Agency used a commercial gateway, but there could be an option for the Digital Agency to manage the node themselves.

・ In addition, it was also discussed that an issue of the right to be forgotten may arise if VCs are also on chain.

D) Initiatives such as trial issuance of NFTs to certify employees' work experience

・ As one of the possible social identities in Web3.0, Soulbound tokens (SBTs), which are linked to accounts, non-transferable, and revocable by the issuer, are advocated as one of the new types of tokens[23]. The list of the token's specific use case includes certification of authenticity of artworks and lending. Some Ethereum Improvement Proposals (EIPs) which may become technological standards for SBTs have been made in the Ethereum community, but none of them have been approved at this point in time.

[23] E. Glen Weyl et al. (2022) "Decentralized Society: Finding Web3's Soul"

- Blockchain Governance Initiative Network (BGIN) is working on in-depth discussions on SBTs for its commercialization. SBTs were initially proposed as a publicly visible token. However, BGIN considers “programmable privacy” as identity that should be realized through SBTs. Accordingly, its discussions assume more advanced use cases such as know your customer (KYC) and know your business (KYB), promotion of tax compliance, diminishing information asymmetry in uncollateralized and other loans, transparent and fair governance, and innovation opportunities[24]. Cases are observed in which non-transferable NFTs are issued by limiting the transferability based on ERC721. Technologically speaking, however, they have issues in realizing the programmable privacy, recoverability, and revocability, and as such, non-transferable NFTs cannot be considered as SBTs. In addition, there remains various points of argument to be discussed in the design, which include incorporation of legal requirements such as the General Data Protection Regulation (GDPR) and life cycle management.
- At BGIN, SBTs are in the phase where a large number of verification tests are being considered. Discussions on various issues and points of argument in the phase will bring SBTs closer to the commercial use. BGIN plans to organize the discussions to issue the paper “Part 2.”

E) International comparison of accounting standards and tax treatment for tokens

- In Japan, after the system for crypto assets was established under the amended Payment Services Act enforced in 2017, the Accounting Standards Board of Japan (ASBJ) issued an accounting standard (Practical Issues Task Force No. 38) in 2018 in response to arguments pointing out that companies cannot receive accounting audit because accounting standards for crypto assets were not yet developed. This accounting standard stipulated the approach in accounting treatment, in which, in the case where a crypto asset is held by a third party other than the issuer, the crypto asset is measured at fair value if there is an active market. Based on the formulation of the accounting standard, crypto assets are measured at fair value for the tax purpose if there is an active market, and the valuation gains and losses are taxable.
- Since then, moves to use tokens as a means for fund-raising have been seen globally. Under such circumstances, Japan’s taxation on crypto assets using the term-end market value “requires tax payment on crypto assets continually held without realized gains associated with cash flows (meaning that they do not have the ability to bear tax), and is pointed out as a factor hindering starting up of business or business development using a blockchain technology in Japan.” For this reason, requests were submitted to revise the

[24] BGIN (2022), “Soulbound Tokens (SBTs) Part 1: Building and Embracing a New Social Identity Layer”

taxation system in FY2023 for the treatment of crypto assets held by the issuers (submitted by the Financial Services Agency and the Ministry of Economy, Trade and Industry).

- In addition, in March 2022, the ASBJ published the points of argument including whether to initiate development of standards for issuance and holding of ICO tokens at this point in time, and solicited opinions on them. At present, discussions are being made based on opinions submitted in response.
- As for the International Financial Reporting Standards (IFRS), views on the holding of certain crypto assets are indicated in the agenda decisions of the IFRS Interpretations Committee (published in June 2019). However, the IFRS do not contain specific descriptions on crypto assets. The final recommendations of the European Financial Reporting Advisory Group (EFRAG)[25] (published in April 2022)[26] present current issues and the future direction on holding and issuance of crypto assets[27]. However, the specific schedule for clarifying the treatment under the IFRS standards has not yet been determined.
- Regarding taxation systems, the Organisation for Economic Co-operation and Development (OECD) considers that, while events of creation and disposal of crypto assets may be discussed as opportunities for imposing tax, storing of crypto assets would not be discussed as such, because the event would not give rise to such an opportunity in general[28]. A study on the U.S., France, Germany, Switzerland, Singapore, South Korea, and Dubai did not find any systems employed to evaluate crypto assets held by companies using the term-end market value.

F) Rights and interests and legal issues concerning various tokens including NFTs

- NFTs are digital data (intangible objects), and it is considered that there are no ideas of ownership and copyrights in NFTs themselves[29]. When a content represented by an NFT is a “work,” the content is protected by the copyright. When NFTs are transferred, copyrights and other similar rights in the content represented by the NFTs are not naturally transferred accordingly. It is necessary to define the legal nature of content represented by

[25] An organization established with missions including introduction of viewpoints of Europe in the development of the International Financial Reporting Standards (IFRS).
[26] RECOMMENDATIONS AND FEEDBACK STATEMENT EFRAG DISCUSSION PAPER ON ACCOUNTING FOR CRYPTOASSETS (LIABILITIES) April 2022
[27] The EFRAG does not recommend to develop independent standards for crypto assets (liabilities) immediately, as such standards are exposed to a risk of being obsolete. Their view is that development of guidance on recognition and measurement of crypto asset issuers by the International Accounting Standards Board (IASB) would become possible after deepening the understanding of rights and obligations concerning transactions through setting of disclosure requirements as well as discussions on issuers’ accounting treatment.
[28] OECD (2020), Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues
[29] Under the Civil Code, subjects of ownership are limited to “tangible objects” (Article 85 of the Civil Code), and NFTs themselves, which are intangible objects, are not considered to be subjects of ownership. In addition, while “work” under the Copyright Act means “a creatively produced expression of thoughts or sentiments that falls within the literary, academic, artistic, or musical domain” (Article 2, Paragraph 1 of the Copyright Act), NFTs are digital data, not a creatively produced expression, and thus it is considered that no copyrights arise in NFTs themselves.

NFTs in the terms of use such other terms, and provisions such as whether copyrights and other similar rights in the content are transferred to the transferees when transferring NFTs should be stipulated.

- Since 2021, the world has shown interest in NFTs in the content area and the market has been vibrant in the short term[30]. On the other hand, however, issues such as damage to consumers caused by illegitimate NFTs and damage to right holders caused by unlicensed NFTs have come to the fore, which are suggested as a hindrance to medium- to long-term development[31]. As part of measures to prevent damage to consumers, the necessity of the following, for example, is pointed out: certification of wallets and contracts under which NFTs are issued, disclosure of information on rights concerning NFTs (license to use content and contract documents regarding secondary distribution)[32], and improvement of consumers' literacy. As part of measures to prevent damage to rights holders, a measure in which the status of infringement of rights including use of unlicensed NFTs was preserved from an objective perspective, was introduced[33].
- In electronic transactions of claims using blockchain technologies, for example, if rights are not perfected against third parties when transferring claims by means of transfer of tokens representing the claims on blockchains, there are risks of being unable to counter such actions as double transfer and attachment. As such, there is a possibility that the stability of transactions is harmed. Regarding this point, under the current law, the assignment of a claim may not be duly asserted against the obligor or any other third party, unless the assignor gives notice thereof, which is made using an instrument bearing a certified date (Article 467, Paragraph 1 of the Civil Code). Content-certified mail or similar instrument is used as an instrument bearing a certified date. In response to the possibility pointed out above, a special provision was established in which, if notice of the assignment of a claim is made by using an information system provided by a business operator certified based on the new business activity plan under the Act on Strengthening Industrial Competitiveness, the notice made through the information system is deemed as notice made using an instrument bearing a certified date (enforced in August 2021). It is expected that discussions on requirements for perfection against third parties make progress amid

[30] The global aggregate market value of NFTs increased about 30 times during the period from June 2021 to March 2022, and after that, dropped about 40% in three months. It has remained flat since then. The recent transaction volume (October 2022) decreased to about over 5% in August 2021 when it hit the peak.
[31] In the questionnaire survey conducted as part of the study entrusted by the Consumer Affairs Agency entitled "Trends in NFTs" (June 23, 2022; Mitsubishi UFJ Research and Consulting Co., Ltd.), 57.8% of the respondents in their 30s answered that "whether it is a fake NFT" is the concern when purchasing and using NFTs. OpenSea, one of the world's largest NFT marketplaces announced on its official Twitter that "Over 80% of the items created (using a tool for creating NFTs provided by OpenSea free of charge) were plagiarized works, fake collections, and spam."
[32] While the general NFT data specifications (ERC721) require name and identifier, where the attribute information such as content is stored, and the holder as the information to be recorded, there are initiatives, for example, to add a recording area for information on rights in content to tokens (Sanpo-Blockchain).
[33] "Initiatives to Establish an Environment for Expansion of Safe and Secure Global Distribution of Japan's Contents NFTs" (October 27, 2022), Japan Contents Blockchain Initiative

the expansion of transactions using blockchains in the future.

- A concern was raised that, in Japan, sale of NFT packages (a form of selling multiple NFTs randomly combining them without making clear what are in the package) and provision of the secondary distribution market for NFTs sold in packages (operated and managed by business operators which engage in package sale) may constitute gambling (Article 185 of the Penal Code). Regarding this point, industrial and other associations have presented their views on the applicability to gambling, upon limiting the scope of application, along with the measures to protect consumers (such as appropriate provision of information on spawn rates and prevention of a large amount of purchasing by minors)[34][35].

[34] The Council for Sports Ecosystem Promotion published the “Guidelines for Combining Sale of NFT Packages Using Sports Contents and Secondary Distribution Market” (September 20, 2022).
[35] Five associated organizations (JCBI, JCBA, JBA, BCCC, and CSEP) published the “Guidelines for Sale of Randomly Combined NFTs” (October 12, 2022).

[Reference 4] Overview of discussions on DAOs

A) Analysis of circumstances of DAOs
B) Recognition of issues related to governance of DAOs
C) Legal position of smart contracts and governance tokens
D) Web3.0 Research Group DAO
E) Vitalization of the content industry and local communities through issuance of NFTs and launch of DAOs
F) Incorporation of DAOs

A) Analysis of circumstances of DAOs

- The results of the analysis of the circumstances of DAOs in Japan and abroad from the following five perspectives: (i) DAOs with a large economic zone; (ii) DAOs that lead to donations and other social contributions; (iii) DAOs for which litigation and other risks have become apparent; (iv) DAO registered in the U.S. State of Wyoming; and (v) DAOs and related business operators in Japan; are as described below.
- **(i) DAOs with a large economic zone**: According to Chainalysis, the 33% of DAOs and the 83% of the treasury balance is related to DeFi[36]. While there are many DAOs focused on venture capitals, infrastructure, and NFTs, the treasury balance is said to be relatively small. (However, the boundaries of these categories are blurred. For example, a venture DAO could be considered DeFi-related.) In addition, according to CoinMarketCap, DeFi-related tokens account for six of the top 10 tokens issued (tagged as a DAO) in terms of aggregate market value[37]. The top 10 tokens are as follows.

	Overview	Overview of related companies obtained from publicly available information
1. Uniswap	Operation of a decentralized exchange	Uniswap Labs (the U.S.) is involved in development and management of protocols and operation of the community.
2. ApeCoin	Operation of BAYC, which is an NFT project	APE Foundation (Cayman Islands) manages ApeCoin based on decisions made by the DAO while Yuga Labs (the U.S.) engages in the development and design
3. Aave	Operation of a decentralized exchange	Aave Limited (the U.K.) has obtained a license as an electronic money business operator
4. BitDAO	Investment in DeFi projects	Unknown
5. MakerDAO	Project management related to stablecoins DAI	DAI Foundation (Denmark) manages intellectual property rights while RWA Company LLC (Cayman Islands) manages investments and concludes contracts
6. Synthetix	Operation of a decentralized exchange	Synthetix (Australia) seems to engage in development functions based on the recruitment status of engineers
7. Dash	Project management related to virtual currency Dash	Dash Core Group, Inc. (the U.S.) engages in development and maintenance of source codes and customer support. All the shares in the company are held by The Dash DAOs Irrevocable

[36] Chainalysis “Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated”
[37] CoinMarketCap (As of November 9, 2022)

		Trust.
8. Curve	Operation of a decentralized exchange	The function of Curve Finance (Switzerland) is unknown.
9. Lido	Building of liquid staking services for Ethereum	Unknown
10. Decred	Project management related to virtual currency DCR	Unknown

- According to the prior research[38], the quorum for governance vote is generally low even if it is a proposal that affects governance, including changes to smart contracts, being 4% for Uniswap (the total number of addresses holding a governance token is about 280,000), 1% for Aave (the same is about 80,000), and 20% for MakerDAO (the same is about 110,000). The overall governance voting percentages (actual result for 2021), including snapshot voting, were about 5-9% for Uniswap, about 4-9% for Aave, and about 2-3% for MakerDAO.
- The purpose of Nouns DAO in which NFT holders have the voting rights concerning the community is to create a community for on-chain avatars. It repeats the process of randomly generating avatars called “Noun” and auctioning one Noun every 24 hours, and stores the full amount of the revenue obtained through the process in treasury, the use of which is determined by the Nouns DAO. It is a fully on-chain NFT which is characterized by the adoption of Creative Commons Zero (CC0; a form in which the creator or owner of the content waives any copyright interest). Under the above system, because the number of initial participants is low, it has been pointed out that it is vulnerable to the risk of malicious proposals, such as undue withdrawal of treasury for personal gain, being made (or voting rights being bought) by participants with a majority of voting rights. In addition, initial members are vested with the refusal right, and a new Noun is presented to them each time 10 Nouns are issued. In hearing sessions conducted by the Research Group, as reasons for why Nouns DAO is functioning, the following were pointed out: firstly, under the DAO, funds from the participants are stored in the treasury, and are used to expand the Nouns community through such ways as provision of assistance to artists, production of a movie featuring Nouns, and provision of funds to create T shirts, and thus the DAO is for non-profit without dividends to participants; and secondly, some of the initial members have demonstrated leadership to smoothly form consensus and make decisions by majority vote. On the other hand, in terms of issues, it was pointed out that there have been cases in which factions were formed within the organization and the organization was internally divided pursuing the acquisition of funds in the treasury, and poor communication

[38] Joint research by the Financial Services Agency and QUNIE CORPORATION, “Report on results of research on technological risks in a trust chain in the decentralized financial system (summary)” (June 2022)

within the community caused discontinuity of communication.

- **(ii) DAOs that lead to donations and other social contributions:** Use cases in overseas countries of DAOs which aim for social contribution include ATX DAO and DAO Charity.
- ATX DAO aims to make Austin, in the U.S. State of Texas, a city that leads Web3.0 economy and to create a close network of crypto asset experts and enthusiasts. In this DAO, tokens are awarded when tasks are performed. The DAO is working on such initiatives as issuing NFTs in partnership with local artists and non-profit organizations, and distributing the sales proceeds among the artists, non-profit organizations, and the DAO.
- The purpose of DAO Charity is to create an international community to support Ukrainian refugees. Collected donations are distributed to each area. The DAO works to ensure the transparency by providing detailed reporting of all means used for donations and the details of expenditures. At this point in time, it has not been confirmed that this DAO implements decentralized governance through the issuance of governance tokens which is considered to be a characteristic of DAOs.
- **(iii) DAOs for which litigation and other risks have become apparent:** Ooki DAO is a case of an organization that has, under the name of DAO, circumvented regulations by conducting business that requires registration without registration. On September 22, 2022, the U.S. Commodity Futures Trading Commission (CFTC) submitted a complaint and issued an order of dissolution against Ooki DAO (bZeroX) and its founder, on the ground that they offered unregistered leveraged trading of digital assets. In this case, one of the CFTC members expressed an opposition that the co-founders are being held liable for the business conducted by the Ooki DAO on the ground that they have participated in voting based on their governance token of Ooki DAO[39]. As such, there have been discussions as to how responsibility should be pursued for the illegal actions of DAOs.
- The DAO incident resulted in a massive unauthorized outflow due to a code vulnerability. The resolution of this issue triggered discussions on how decentralized governance of blockchains should be. The DAO was a project, the purpose of which was to build a decentralized investment fund by using smart contracts on an Ethereum platform. In 2016, a hacker identified a vulnerability in the DAO's program code. This resulted in an unauthorized outflow in the form of funds held by the DAO being transferred to another address. As a result of discussions on actions to be taken, the decision was made to use the hard fork technique in which the hacked transaction itself was to be nullified after tracking records on the Ethereum blockchain (the decision required approval by at least half of the Ethereum community participants). The implementation of the hard fork triggered discussions on how the decentralized system of Ethereum itself should be.

[39] https://www.cftc.gov/PressRoom/SpeechesTestimony/mersingerstatement092222

- **(iv) DAO registered in the U.S. State of Wyoming:** In the U.S. state of Wyoming, a state law defining DAOs as LLCs went into effect on July 1, 2021 (the details of the state law are as described below). Specific examples of DAOs registered under said law are as follows.
  - Fries DAO: Its purpose is to acquire fast food stores. It is said that the DAO offers stable coins to purchasers of stores, instead of the actual ownership, and seeks a method of allowing them to collect funds by being involved in the decision-making process. In October 2022, it was reported that this DAO has become a victim of a hack in which tokens equivalent to 2.3 million dollars (320 million yen) was stolen[40] (the operator also tweeted about the fact of the damage). For the wallets of the developers of this DAO, Profanity, which is a wallet generation tool and has been known to have a serious security flaw, was used.
  - Kitchen Lands DAO: The DAO is purchasing land and conducting other demonstrations with the aim of acquiring and managing assets through a decentralized community.
  - American CryptoFed DAO: It is said that the DAO intends to conduct promotion of the stablecoin Ducat to realize transactions without fees based on EOS, under the mission of creating a currency system with zero inflation, zero deflation, and zero transaction costs.
  - BLOCKS DAO: The purpose of the DAO is to provide solutions such as Verified by BLOCKS (VbB; which can be used for secure trading, tracking and settlement of digital and physical assets).
  - Elo DAO: The purpose of the DAO is to lower crypto liquidity risks by providing DeFi (claims).
- **(v) DAOs and related business operators in Japan:** In Japan, the possibility of use of DAOs as a tool for solving various social issues has been pointed out. Example cases include a DAO which aims to improve the voting percentages of younger people[41] and a DAO which aims to solve issues in the local community (such as Yamakoshi and Shiwa-cho for which the Web3.0 Research Group conducted hearing sessions).

B) Recognition of issues related to governance of DAOs

- According to the prior research[42], issues such as the following have been pointed out for governance by voting at DAOs: a low quorum for voting, low voting percentages, difficulty in verifying malicious proposals, and the possibility that changes to smart contracts are not properly understood. The following issues have been confirmed for cases described in

[40] crypto.news, "FriesDAO Hacked for $2.3 Million in the Latest Profanity Exploit," October 29, 2022 https://crypto.news/friesdao-hacked-for-2-3-million-in-the-latest-profanity-exploit/
[41] https://www.dot-jp.or.jp/news/pressrelease/15148.html
[42] Joint research by the Financial Services Agency and QUNIE CORPORATION, "Report on results of research on technological risks in a trust chain in the decentralized financial system (summary)" (June 2022)

"Analysis of circumstances of DAOs" (in A above).

- A related party of an organization preparing a DAO may utilize the DAO to circumvent regulations.
- The ownership of responsibility of DAO participants in the event of trouble is unclear.
- A participant with malicious intent may obtain a majority of governance tokens and exercise the voting right for their own benefit.
- Strong rights including a refusal right given to certain members such as founders to address these issues could undermine the decentralized nature of the operation.

C) Legal position of smart contracts and governance tokens

- Usually, smart contracts are considered to be an automatic enforcement protocol for pre-agreed contracts rather than the contracts themselves. Accordingly, for example, even in services that use smart contracts such as DeFi, the protocol itself which consists of smart contracts does not usually constitute a contract, but is considered to be only an automatic enforcement of the agreed terms in the contract. Cases where it is difficult to use smart contracts include contracts involving intentionality, negligence, and other legal evaluations, and contracts that would violate consumer protection laws and other laws and regulations or offend public order and morals if automatically enforced. In addition, points of attention regarding smart contracts in practical use, such as the possibility that incorrect data which is input from the outside may produce a result that is different from what is originally intended, still need to be verified in various use cases.
- A governance token, which can be said to be a core element of DAOs, is a generic term for a token that represents a voting right. In this context, in Japan, it is considered that the legal position of governance tokens is not directly affected by the fact that the tokens represent voting rights. In reality, however, many governance tokens have the nature in that they can be freely exchanged for crypto assets. Therefore, discussions on the applicability to crypto asset arise. On the other hand, there have been some cases where voting rights are attached to NFTs, as seen in Nouns DAO. As with other NFTs, in Japan, the legal position of these cases is considered to be unclear.

D) Web3.0 Research Group DAO

- A member of the Research Group proposed to launch a DAO of the Research Group, and the DAO was established separately from the Research Group itself, upon agreement by the Research Group.
- The Research Group DAO began as a voluntary organization based on a voluntary will of the Research Group members and the secretariat, not led by the Digital Agency secretariat, to aim for decentralized governance which is one of the characteristics of DAOs.

- The purpose of establishing this DAO is to allow members to ascertain issues and possibilities through experience as users of DAO and promote deeper discussions by the Research Group.
- As the period from the agreement to establish the DAO to the creation of the report was only about a month and a half, only minimal functions such as issuance of original tokens, voting, and discussions using chat tools are implemented in this DAO.
- More specifically, the following initiatives have been undertaken.
  - A chat tool, Discord, is used for communication between members so that they can share information and exchange opinions at any time.
  - Governance tokens are issued to members in the form of non-transferable NFT. Decisions are made through voting within the community.
- Through this initiative, the following points of argument and issues have been identified:
  - Legal issues related to administrative bodies having crypto assets;
  - An appropriate means to obtain tokens when the Layer 2 protocol is used;
  - How tokens for the operation purpose are collected from DAO members; and
  - Variances in the proficiency level of and frequency of access to the communication tool
- The following opinions have been raised from the members regarding the future possibilities.
  - More diverse opinions may be gathered if the number of participants in the DAO increases.
  - It may be good that contributions to the Government remain by issuing non-transferable NFTs.

E) Vitalization of the content industry and local communities through issuance of NFTs and launch of DAOs

- With regard to vitalization of the content industry through Web3.0, while various IP business operators announce their entry into the Web3.0 business, Blitmap demonstrates itself a case of content co-creation by a community. Blitmap adopts a Creative Commons Zero (CC0) policy, and therefore waivers copyrights for the purpose of promoting new creation by the community, including secondary work. It is argued that the attempt to create and develop content in a decentralized manner is different from the conventional approach of creating and developing content while protecting them with copyrights.

F) Incorporation of DAOs

- Incorporation is a major point of argument when considering the legal position of DAOs.

Generally speaking, it is said that establishing a legal entity to launch or manage an activity can be expected to have advantages such as that (1) the responsibility of natural persons involved can be limited to limited liability; (2) commercial transactions such as opening bank accounts and executing contracts can be facilitated; and (3) licenses required for regulated businesses can be obtained. As such, incorporation of DAOs and the legal position of DAOs as a prerequisite for such incorporation are important issues to be addressed when considering rights and obligations of DAOs and people involved in them.

- Under such circumstances, the U.S. State of Wyoming enforced a state law which defines DAOs as LLC[43] (hereinafter, the "DAO Act") on July 1, 2021[44]. The DAO Act defines the requirements for incorporating DAOs, registration procedures, rights and obligations of members, and reasons for dissolution. In addition to having the characteristics of a regular LLC, DAOs are designed with blockchain-based organizational operations in mind. The Act requires DAOs to describe the smart contract identifiers that will be directly used to manage, promote, and operate the DAO, the algorithm used in the operation, and the role played by the participants in their articles of incorporation.

Position of the DAO Act	・ The so-called DAO Act refers to regulations related to DAOs based on Chapter 31, which were newly created in Title 17 of the Wyoming State Law. ・ In the DAO Act, a "DAO" is defined as a "limited liability company incorporated based on the provisions in this chapter." ・ The DAO Act is positioned as a special provision attached to the limited liability company law of the State of Wyoming, and said law is applied to DAOs to the extent consistent with the provisions of the DAO Act.
Requirements for incorporating DAOs	・ The requirements for incorporating DAOs based on the DAO Act are stipulated in Title 17, Chapter 31, Article 104 onwards of the Wyoming State Law. For example, it requires DAOs to include the following matters in the articles of incorporation: 1. that it is a DAO; 2. fixed phrases to the effect that DAOs may be, unlike regular limited liability companies, subject to certain restrictions, such as fiduciary duty of equity holders, disposal of rights held, and withdrawal; 3. smart contract identifier directly used for management, promotion, and operation of the DAO; 4. matters related to how participants operate the DAO, including to what extent the DAO will be operated in accordance with the algorithm; and 5. matters related to the DAO, such as rights and obligations of the participants, details of activities of the DAO, dividends paid before withdrawal or dissolution, and changes to the articles of incorporation. ・ It is required to include "DAO," "LAO," or "DAO LLC" in the name of the DAO. ・ A DAO can be incorporated by submitting the articles of incorporation to the Secretary of State and with only one member.
Registration procedures for DAOs	・ In order to register a DAO as a corporation, it is required to input and submit necessary information online or use a paper form. ・ The registrant may not necessarily be a resident of the State of Wyoming, but to register a DAO, a registered agent who meets certain requirements including having an address in the State of Wyoming is required. ・ It is not permitted to register a DAO of a foreign country as a DAO under the DAO Act.

[43] LLC: Limited Liability Company
[44] https://www.wyoleg.gov/Legislation/2021/SF0038

Rights and obligations of members	・ While members bear duty of good faith, they are not subject to fiduciary duty. ・ Members do not have the right to request permission to inspect financial and other documents, as long as such documents are published on an open blockchain
Withdrawal of members	・ The conditions and procedures related to withdrawal of members are stipulated in either the articles of incorporation, smart contract or operation contract. ・ If there are no special provisions in the foregoing, a member will withdraw from the DAO when they transferred all property underlying their equity interest, voting right, or economic right
Dissolution of DAOs	・ Reasons for dissolution of DAOs shall be as follows: 1. when the duration of the DAO expires; 2. when a resolution for the dissolution has been passed by the majority vote of the members; 3. when a reason for dissolution stipulated in the smart contract, articles of incorporation or operation contract has occurred; 4. when the DAO approved no proposal or conducted no activities for a period of one year; or 5. when the DAO ceased to have a legitimate business purpose or there is no longer a single natural person member 6. (vi) when all of the members of the DAO have withdrawn.

[Reference 5] Overview of discussions on decentralized identity (DID)

A)	**Functions and role played by decentralized identity**
B)	**Use cases**
C)	**Developments in technologies and standardization**
D)	**Discussions on the relationship with personal information protection in various other countries**
E)	**Combination of decentralized identity and keys for My Number cards and issues thereof**
F)	**Decentralized identity in corporations**

A) Functions and role played by decentralized identity

- In prior research,[45] the following concepts have been identified:
  - Self-sovereign identity (SSI): A concept in which individuals are allowed to control their own identity without the intermediation of an identity administrator
  - Decentralized identity (DID): A mechanism in which the degree of reliance of users' identity on identity providers is lowered so that such identity does not rely on specific identity providers
- The main advantages expected from DID are that (i) it allows users to manage their own personal information, which has previously been held by administrative organs and/or specific private-sector business operators, to ensure greater protection of such information; (ii) it allows for a higher level of security by eliminating single points of failure by not having a specific administrator in place; and (iii) it simplifies identity authentication in domestic, overseas, and digital spaces by increasing the interoperability among various services.
- The main technologies that realize DID include verifiable credentials (VCs) and decentralized identifiers (DIDs).
  - VC: A certificate which can be disclosed at the will of the user and verified, which was standardized by the World Wide Web Consortium (W3C) in November 2019.46 Approaches to realize this technology include ensuring the confidentiality and authenticity of personal attribute information by using public key encryption and presenting the public keys of the issuer and user, as well as the encrypted certificate, to the verifier.
  - DIDs: It was standardized by the W3C in July 2022,47 and defined as an identifier which does not require the intervention of any centralized registration organization. In

[45] Nomura Research Institute, Ltd., "Research on the use of digital identity using blockchain technologies," March 2021 https://www.fsa.go.jp/policy/bgin/ResearchPaper_NRI_ja.pdf
[46] The updated version of this standard, V.1.1, was published in March 2022. (Source) https://www.w3.org/TR/2022/REC-vc-data-model-20220303/
[47] (Source) https://www.w3.org/TR/did-core/

the W3C's discussions, specifications utilizing blockchains were envisioned. On the other hand, cases have been observed in which specifications that do not use blockchains are being considered from perspectives such as protecting personal information. This technology is utilized to identify the issuer and verify authenticity using a public key when issuing and verifying VCs.

- One of the envisioned future concepts of Web3.0 is the possibility of DID being used as a new ID that is highly interoperable and can be used in a variety of domestic, overseas, and digital spaces. In light of this, one possible case of practical application of DID in Japan is digital ID wallets in which My Number-related information can be used as VCs. On the other hand, there are major issues in realizing the foregoing, which include: (i) how to realize collaboration among governmental services Japan (such as My Number cards and Mynaportal); (ii) how public keys, which are generated when issuing certificates taking personal information protection into consideration, should be managed and transmitted; and (iii) how certificates and private keys held by individuals are managed, and what actions should be taken in cases of loss or unauthorized use of them.

B) Use cases

- Although services based on VCs and DIDs are being considered in anticipation of ensuring global interoperability, at present, utilization of these technologies are being considered mainly in public services and digital ID services for administrative purposes, and there are limited cases of such technologies being used by the private sector, for reasons such as that technologies related to DID are still under development, data that falls under the category of personal information as well as rules for its handling and protection have not yet been established, and it is not easy to secure revenue from certification services. In addition, even in public and administrative services, DID is merely one of the options among technologies to be used.
- Specific examples of initiatives are as described below.
  - EU: The establishment of EU digital identity wallets is being considered, with the aim of collaboration with the ID services of EU member states and improving the convenience of procedures (e.g.: driver's license, degree certificates, electronic prescriptions, payments, and online signatures) within the EU zone, and rules and technological specifications for various use cases are being formulated and a demonstration experiment[48] is being conducted. On the other hand, whether VCs and DIDs will be used in commercial services has not yet been determined.

[48] Four organizations (EUDI Wallet Consortium (EWC), Nordic-Baltic eID Project (NOBID) Consortium, The PilOTs for EuropeaN digiTal Identity wALlet (POTENTIAL), and Digital Credentials for Europe (DC4EU)) have been promoting the demonstration experiment since August 2022.

- In Canada, Interac Verification Service (former Verified.me) has been considering the use of VCs and DIDs in commercial endeavors in 2023. Verified.me shares identity verification information used at the time of opening a bank account by a user at his/her discretion and thereby facilitates the identity verification necessary at the start of using insurance and administrative services, and is promoting system development for VCs and DIDs toward further improvement of interoperability, with the aim of realizing collaboration with various domestic and international services. In addition, the Digital Identification and Authentication Council of Canada (DIACC) formulates rules necessary for transferring personal information, as well as rules that business operators who provide the system for the transfer are required to follow.
- Other examples in which VCs and DIDs are used: The U.S. State of New York has provided, jointly with IBM, "Excelsior Pass," which is a mobile app to certify that the holder has received COVID-19 vaccination and/or has been tested negative in a PCR test. The U.K. National Healthcare Service (NHS) has developed, jointly with Microsoft and other vendors, "NHS Staff Passport" to certify occupational history and qualifications of healthcare professionals.

C) Developments in technologies and standardization

- As described below, multiple organizations are moving forward with discussions toward standardization. For example, the W3C published documents concerning standardization of VCs in July 2019 and DIDs in August 2022. In addition, the Decentralized Identity Foundation (DIF) and the Hyperledger Foundation have been developing systems based on various specifications for VCs and DIDs.
- The following issues with putting them into practical application have been identified.
  - Ensuring interoperability: While there are more than 100 types of DID methods,[49] ensuring the interoperability of each method has been an issue. Libraries of DID methods for each blockchain are being developed (such as "Universal Resolver" of the DIF) so that digital signatures issued in a blockchain can be read in another blockchain.
  - Standardization of key management: Various development communities are discussing how private keys should be managed safely by individuals and how such keys can be recovered in the case of loss. However, the DIF and the Hyperledger Foundation are taking different approaches and no standardized method has yet been established.

[49] A DID method is a definition of how DID is generated, renewed, and deleted in a specific blockchain. For more details, refer to "Decentralized Identifiers (DIDs) v1.0" of the W3C. As of November 29, 2022, 136 DID methods are registered in the note "DID Specification Registries" issued by the W3C.

D) Discussions on the relationship with personal information protection in various other countries

- When the W3C was standardizing DIDs, the use of blockchains (public blockchains in particular) was envisioned in anticipation of ensuring interoperability and the elimination of single points of failure. On the other hand, the possibility that identifiers and public keys may constitute personal information has been discussed mainly in Europe, and various actions have been observed in which information recorded on blockchains is limited and detailed information is linked individually by means other than blockchains, or in which blockchains are not used, in order to avoid personal information being made public. At present, business operators are seeking different approaches, and standardization and establishment of methods in the future are being awaited. More specifically, the following methods are being considered. In each case, intervention by a business operator is required to a certain degree, which may make it difficult to eliminate a single point of failure.
  - In the Sovrin Network used in NHS Staff Passport, decentralized identifiers and DID documents of individuals are not recorded on a blockchain but are directly transmitted through communication between an individual and the verifier.
  - While Microsoft provides Microsoft Entra Verified ID as a solution for VCs and DIDs, it provides services which use blockchains and services that use normal cloud servers.
  - In addition, there are cases in which viewing of data is restricted by limiting the blockchain node hosts to only specific business operators that are qualified to handle personal information.

E) Combination of decentralized identity and keys for My Number cards and issues thereof

- As a way to use information held by administrative bodies in DID, it may be possible to issue information obtained through Mynaportal as VCs so that users can manage their certificates and provide their attribute information selectively, at their own discretion.
- For example, it may contribute to improved convenience for users if it is possible to collect, using Mynaportal's self-information collection API, information that users can manage themselves on Mynaportal, collect information from the private sector (through methods to be separately considered), and centrally manage such information in users' digital ID wallets.
- On the other hand, it should be noted that My Number cannot be used as an identifier for purposes other than social security, tax, and disaster control measures, and it is difficult to use basic information on My Number cards as VCs.
- In addition, the following issues have been pointed out for cases where digital ID wallets

are established using VCs or DIDs, and it may be necessary to consider these points from a long-term perspective.

- Registry management: There is still no established approach to how to balance the elimination of single points of failure (improvement of security) and the protection of personal information and privacy through use of blockchains, and it is necessary to consider the appropriate balance while paying attention to the status of initiatives in various countries and developments in technologies, among other things.
- Private key management: Discussions on technologies and standardization of private key management are still underway. In many existing services, cloud services such as AWS and Azure or the issuers of certificates manage private keys, which allows single points of failure to remain. It is necessary to discuss how users manage their own private keys and how to recover private keys when they are lost, while keeping an eye on advances in key management, encryption, and other technologies.

F) Decentralized identity in corporations

- It is considered easier for corporations to promote DID, because they have relatively minor concerns about personal information and privacy and they have an increasing demand to link information in a manner that guarantees confidentiality and authenticity to business operators, due to recent regulations and other rules related to supply chains.
- The U.S. “Drug Supply Chain Security Act” (DSCSA) to be enforced in November 2023 requires submission of information on the drug manufacturing process in a saleable package unit. Preparations are also being made to enforce regulations which require reporting of product information on EV batteries sold within the EU.
- Spherity provides drug and EV battery traceability services for supply chain-related business operators using VCs and DIDs. In addition, these services are provided using blockchains such as Ethereum as the system infrastructure.

[Reference 6] Overview of discussions on user protection and law enforcement

A) Circumstances of crimes related to crypto assets
B) Complaint analysis by authorities
C) Establishment of systems in investigative organizations in the U.S.
D) Developments in RegTech/SupTech and the possibility of collaboration with law enforcement authorities

A) **Circumstances of crimes related to crypto assets**

- According to the "Chainalysis 2022 Crypto Crime Report"[50] issued by Chainalysis, the amount of damage in 2021 totaled 14 billion dollars (an approximate 79% increase compared to the previous year). The areas with the largest amount of damage are (i) fraud (about 7.7 billion dollars), (ii) thefts (about 3.2 billion dollars), and (iii) darknet market (about 2.1 billion dollars).

  Fraud

  - There have been an increasing number of cases of exploitation by rug pull (a technique used to deceive customers and collect funds for development and other purposes and then to withdraw pooled funds). Among the top 15 cases in 2021 where damage was caused by rug pulls, 14 cases occurred in DeFi. Crimes related to DeFi are rapidly increasing. It has been pointed out that, in DeFi, by intentionally implementing vulnerable smart contracts, developers are able to raise funds and then improperly withdraw them.
  - AnubisDAO, which was launched on October 28, 2021, disclosed a plan to provide a decentralized floating exchange rate currency with financial evidence. AnubisDAO, which did not have a website or white papers, and was comprised only of developers using pseudonyms, raised funds of almost 60 million dollars from investors in one night. All investors received an ANKH token in exchange for providing funds to the liquidity pool of the project, but only 20 hours later, the funds raised and pooled in Anubis DAO's liquidity pool were transferred to multiple new addresses.

  Thefts

  - Among the top 10 large-scale thefts of crypto assets that occurred in 2021 and the first quarter of 2022, seven cases occurred in DeFi. DeFi has the characteristics of making smart contract codes public. As such, it is easy for criminals to analyze and hack the codes, and in many cases, attacks are made utilizing smart contract

[50] https://go.chainalysis.com/crypto-crime-report-2022-jp.html

vulnerabilities, or techniques of flash loans[51] are used. In addition, cases of damage occurred in which private keys or accounts related to crypto assets of customers were stolen through phishing or social engineering, and crypto assets are withdrawn from customers' wallets.

- On August 11, 2021, at Poly Network (a project which enables the interoperation of different blockchains), a hack targeting its smart contract vulnerabilities occurred and crypto assets worth 612 million dollars were stolen.[52]

Darknet market

- Darknet market include the drug market (sales of at least 1.8 billion dollars) and sites (sales of about 0.3 billion dollars) that sell stolen login and credit card information, exploit kits[53], and other illegal data.
- About 80% of sales in the darknet market were accounted for by the Hydra Market, which provides services to Russian-speaking countries and regions. On April 5, 2022, the U.S. Department of Justice and the Criminal Police Office of the Federal Republic of Germany conducted joint crackdowns and attached bitcoins worth 25 million dollars and operating servers, forcing the market to close.

Other crimes including money laundering

- Other crimes include ransomware,[54] malware,[55] transactions subject to sanctions (such as those with North Korea, Russia, and Iran), terrorism financing, and crimes related to NFTs.
- Crimes related to NFTs include, in addition to fraud and theft, wash trade[56] (about 8.5 million dollars) and money laundering through the purchase and resale of high-priced NFTs such as digital art (about 1.4 million dollars).
- Chain-hopping,[57] mixing,[58] and anonymity enhanced cryptocurrencies[59] (AECs) are

[51] This is a function of the DeFi protocol which enables borrowing of crypto assets, tokens, and other such assets without collateral, and in which the processing and repayment of debts can be completed within the same transaction (transaction on one chain such as Ethereum). While it is highly convenient, there is a risk that this function enables a borrower to borrow funds in a large amount, purchase a large amount of assets using the funds, causing the price of assets to rise, and sell the assets at a higher price.
[52] At a later date, the hacker returned almost all of the funds stolen, stating that the purpose of the attack was to hack, not to steal.
[53] These are hacking tools used by cybercrime offenders exploiting vulnerabilities of PCs and devices.
[54] This is a criminal technique in which criminal offenders steal data of companies and other entities and demand a ransom.
[55] This is the use of virus software and other such means to withdraw funds from customers' wallets or to conduct unauthorized mining from customers' devices.
[56] It is a technique in which multiple traders concurrently place buy and sell orders using the same trader ID or account to intentionally the raise value of NFTs.
[57] It is a technique in which transactions of converting a crypto asset to another are conducted in a complex and swift manner.
[58] Anonymization of sources and recipients of remittance and transaction data by mixing crypto asset transactions data of multiple sources and recipients.
[59] Ring signatures and stealth addresses are used for anonymization. The list of currencies includes Monero. https://www.getmonero.org/

used as methods of transferring criminal funds, making the tracing difficult.

- Basically, it is necessary to conduct identity verification in compliance with the AML/CFT regulation when engaging in financial transactions and crypto assets transactions. However, many cases are observed in which transactions are carried out without undergoing strict screening, by conducting transactions using crypto asset exchanges, non-custodial wallets, and other similar means that are not compliant with the AML/CFT regulation.

B) Complaint analysis by authorities

- According to a report by the U.S. Consumer Financial Protection Bureau (CFPB),[60] about 8,300 complaints were filed during the period from October 2018 to September 2022. Looking at the breakdown, the most common cases are fraud and theft (40%), which are followed by complaints related to transactions such as those concerning fees and those stating that transactions could not be carried out real-time (25%), and inability to withdraw customers' assets due to bankruptcy or frozen accounts of operating companies (16%).
- In regard to damage from fraud and theft, various types of fraud were reported, such as romance scams, pig butchering,[61] and fraud disguised as influencer or customer services. In addition, cases were observed in which customers' private keys or wallet accounts were stolen using such means as SIM swap[62] hacking, phishing attacks,[63] and social engineering.[64]
- In many of the above cases of fraud and theft, operating companies reportedly held customers responsible for management of their own accounts and did not accept requests for compensation or refunds for damage.
- In light of such damage, the CFPB and the Federal Trade Commission (FTC) provided online resources[65] to help consumers to avoid fraud and theft related to crypto assets.
- In Japan, the number of inquiries received by the National Consumer Affairs Center of

---

More detailed information is provided in "Research and Study on Privacy Protection and Traceability in Financial Transactions Using Blockchains" issued by the Financial Services Agency and Mitsubishi Research Institute, Inc. (https://www.fsa.go.jp/policy/bgin/ResearchPaper_MRI_ja.pdf)

[60] https://files.consumerfinance.gov/f/documents/cfpb_complaint-bulletin_crypto-assets_2022-11.pdf

[61] This type of fraud is called "pig butchering," likening the fraud process to the process of raising and then butchering pigs. It is a technique in which criminal offenders build relationship of trust with victims using such means as social media, solicit purchase of assets such as crypto assets, temporarily allow the victims to gain profit to make them feel comfortable, and then, finally, cheat the victims out of their money.

[62] SIM swap is a technique to improperly manipulate systems of communication carriers and to transfer the telephone number targeted for the attack to the SIM card of the smartphone held by the hacker. The hacker obtains a certification code via a short message service and becomes able to conduct various operations on the victim's wallet using the account of the victim as if he or she is conducting such operations.

[63] It is an online fraud technique in which emails or such other messages are sent from a source disguised as a trustworthy sender to many and unspecified recipients or specific targets to swindle IDs and passwords, credit card numbers, personal information, property, or trade secrets

[64] This is a collective term for techniques used to steal passwords or password prompts by contacting or approaching the data subject or people around the data subject who know such information

[65] https://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf
https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

Japan during the period from 2019 to 2021 totaled 12,498, and damage from fraud such as investment solicitation and romance scams were indicated as the most common cases. The numbers of inquiries related to NFTs[66] were four in FY2020 and four in FY2021, respectively. Activities to call attention to problems related to crypto assets included creation of attention-getting posters through joint efforts of the Financial Services Agency, the Consumer Affairs Agency, and the National Police Agency and introduction of consultation desks.

C) Establishment of systems in investigative organizations in the U.S.

- In the U.S., law enforcement agencies such as the Department of State, the Department of Justice (including the National Security Division, Federal Bureau of Investigation, Drug Enforcement Administration, and U.S. Marshals Service), and the Department of Homeland Security (Homeland Security Investigations and U.S. Secret Service), as well as supervising bodies such as the Department of the Treasury (Financial Crimes Enforcement Network and Office of Foreign Assets Control), the Securities and Exchange Commission, and the Commodity Futures Trading Commission, are working on initiatives for prevention and investigation of crimes related to crypto assets.
- A report issued by the U.S. Department of Justice[67] lists issues such as the following: (i) anonymity in transactions related to crypto assets makes crime investigation difficult; and in addition, in cases of cross-border crime, (ii) it is difficult to collect sufficient information from the country and/or business operators of the country for reasons such as regulations, and (iii) investigation will be hindered when the investigative authority of the country has low crime investigation capability. The following initiatives have been undertaken to address such problems.

  <u>Creation of specialized teams</u>

  - Organizations specializing in blockchain technologies are newly created for purposes such as enhancement of investigational capabilities, cross-departmental information sharing, and education.
  - The Department of Justice established the National Cryptocurrency Enforcement Team (NCET) in October 2021, which identifies, examines, supports, investigates, and prosecutes criminal misuse of digital assets. The NCET sets strategic priorities related to digital asset technologies, works on problems arising from the application of existing laws to new ways of using digital assets, and leads the initiatives of the Department of Justice to cooperate with law enforcement agencies, regulatory bodies, and private-

[66]The Consumer Affairs Agency, materials from the “45th Internet Consumer Transactions Liaison Meeting”
[67] “How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets” https://www.justice.gov/ag/page/file/1510931/download

sector companies in the U.S. and other countries to prevent criminal use of digital assets.

- The Digital Asset Coordinator (DAC) network was established in September 2022 under the leadership of the NCET. The DAC is comprised of federal prosecutors designated by the U.S. Attorney's Office and the litigation department of the Department of Justice. The DAC network provides its members with opportunities to acquire best practices in relation to the examination, analysis, and crime investigation of new fields such as DeFi, smart contracts, and token-based platforms, and aims to increase the number of digital asset specialists.
- The Federal Bureau of Investigation established the Virtual Asset Unit (VAU) in March 2022. The VAU centralizes the FBI's expertise in cryptocurrencies and provides training on technology equipment, blockchain analysis, and digital asset seizures, as well as other advanced cryptocurrency training to FBI employees. The FBI has already trained thousands of FBI employees and partners around the world using this curriculum.

Information provision at international conferences

- The U.S. signed an additional protocol of the Budapest Convention[68] and is working to improve the cooperative system for information collection for criminal investigations. This has enabled the U.S. to more easily obtain information on domain registrations and internet subscribers and traffic data retained by service providers in countries other than the U.S. In addition, the U.S. is promoting the conclusion of not only multilateral agreements but also a bilateral treaty on legal assistance in criminal matters (Mutual Legal Assistance; MLA).[69]
- The U.S. participates in the international Financial Action Task Force (FATF) and the International Organization of Securities Commissions (IOSCO), and is actively exerting influence over them.
- The U.S. Department of the Treasury and others participate in the FATF. The Department co-chairs the Virtual Assets Contact Group (VACG). The U.S. is striving to reduce crimes related to crypto assets by strengthening monitoring of AML/CFT regulation, crypto assets, and virtual asset service providers (VASPs), and by encouraging various countries to comply with the FATF recommendations.
- The Securities and Exchange Commission and the Commodity Futures Trading Commission participate in the IOSCO. The IOSCO serves as a venue for sharing

[68] International convention to globally address computer crimes and cyberattacks, which was adopted in 2001. On May 12, 2022, the signing ceremony for the additional protocol was held at the headquarters of the Council of Europe in Strasbourg, France.
[69] As of April 2022, 74 countries, regions and islands have entered into the treaty. https://www.justice.gov/criminal-oia/file/1498806/download

information and experience on regulatory proposals beyond jurisdictions and new practice, with the aim of minimizing risks on arbitrage transactions within the jurisdictions and market fragmentation for stablecoins, crypto assets, DeFi, and cryptocurrency derivatives and other instruments.

Training provided to investigative authorities of various countries

- The U.S. is implementing some major initiatives which aim to make use of its own expertise in examining digital assets and to promote sharing of expertise with the counterparts of other countries through training and exchange of case-specific information.
- The Global Law Enforcement Network, which is managed by the Department of State and the Department of Justice (Federal Investigation Division), is comprised of advisor attorneys-at-law of the Department of Justice who are assigned across the world and specialize in areas such as international computer hacking, intellectual property, crypto assets, and the dark web. The Network conducts drills and provides technological support related to cybercrime for law enforcement agencies, prosecutors, and judicial partners in countries in Southeast Asia, Eastern Europe, and Central and South America.
- At the Department of Justice, NCET members have provided various types of international training on digital asset prosecution for groups such as the Criminal Affairs/Legal Affairs Sub Group of the G7 Rome-Lyon Group,[70] U.S. and European Cryptocurrency Working Groups, the European Prosecutor Meeting of the Council of Europe, and the Virtual Currencies Meeting of the Europol. In addition, the VAU, under the Federal Bureau of Investigation, has developed the aforementioned training programs and provides them to investigative authorities of various other countries.

D) Developments in RegTech/SupTech and the possibility of collaboration with law enforcement authorities

- The role played by RegTech/SupTech business operators in the prevention and investigation of crimes is significant. The results of hearing sessions conducted with business operators monitoring crypto asset transactions and e-KYC business operators on issues, initiatives, and other such matters related to the circumstances of their services and prevention and investigation of crimes are as described below.

Monitoring business operators

- Business operators monitoring crypto asset transactions, such as Chainalysis, Elliptic, and NiceActimize, examine and analyze records and flows of crypto asset transactions

[70] This is a joint meeting of the Rome Group, which is comprised of specialists on measures against international terrorism, and the Lyon Group, which is comprised of specialists on measures against international organizational crimes of G7.

as well as which addresses are linked with what organizations, and observe the circumstances of crypto asset transactions.

- The above tools are actively used in the U.S. as well, and it has become possible to identify and trace transactions in many major blockchains. In addition, by combining these tools with external ones, such as transaction filtering services and open source tools, it has become possible to identify attributes of organizations and individuals who are involved in the transactions.[71]
- New technologies are developed daily through using machine learning, automation technologies, and other such technologies to address new threats such as advancement of criminal techniques, including money laundering, that make use of mixing services or DeFi. In addition, enforcement authorities in the U.S. have prohibited and cracked down on the use of concealment services.[72]

E-KYC business operators

- E-KYC service providers such as Liquid provide online identity verification services to business operators who are subject to the AML/CFT regulation (specified business operators who are subject to the Act on Prevention of Transfer of Criminal Proceeds).
- The identity of users of wallets used by crypto-asset exchange service providers who are specified business operators is made clear under information management by specified business operators; therefore, verification of such identity is fully compliant with the AML/CFT regulation. However, unhosted wallets used in services such as DeFi can execute transactions without making the identity of the users clear, and thus have issues related to the prevention and investigation of crimes.
- It has been pointed out that there can be a scenario in which a technological and systemic infrastructure[73] will be established in the future, which will enable individuals to hold their own identity verification information and present such information to regulatory authorities when necessary, so that identity verification is made possible in services such as DeFi, which are operated in a decentralized manner.

[71] (Source) U.S. Department of Justice "The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets" (September 16, 2022)
[72] The U.S. Office of Foreign Assets Control (OFAC) sanctioned one of mixing service providers, Tornado Cash, on August 8, 2022, and the developer was arrested for allegedly assisting with money laundering.
[73] Decentralized identity addressed in Chapter 3 can serve as this technological infrastructure in such circumstances.

[Reference 7] U.S.: Overview of the report on the six key priorities identified in the "Executive Order on Ensuring Responsible Development of Digital Assets" (March 2022) (announced on September 16, 2022)

1. Protection of consumers, investors, and businesses		
Digital assets could pose significant risks to consumers, investors, and businesses. The prices of these assets are highly volatile, and the global aggregate market value of cryptocurrencies at present is about one0third of the peak hit in November 2021. It is still customary for sellers to make misleading statements on the characteristics of and expected returns from digital assets, and in many cases, they do not comply with laws and regulations. According to a study, about one-fourth of digital coin offerings are found to have problems with information disclosure and transparency, such as plagiarism of documents and false promises regarding guarantee of returns. Fraud, fraudulent business practices, and theft in the digital asset market are increasing. According to the statistics of the FBI, monetary losses caused by digital asset fraud reported in 2021 increased by 600% year over year. The current administration and regulatory authorities have worked to ensure consumer protection and fair transactions in the digital asset market by issuing guidance, increasing the number of enforcement personnel, and engaging in active questioning of persons who conduct fraudulent acts. The administration plans to take the following additional measures:		
Active promotion of investigations and enforcement actions against illegal acts in the area of digital assets	Securities and Exchange Commission Commodity Futures Trading Commission	(ii)
Doubling initiatives toward enforcement against unfair, fraudulent, or illegal acts based on consumer complaints monitored	Consumer Financial Protection Bureau Federal Trade Commission	(ii)
Formulation of guidance and such other documents related to risk treatment for the digital asset ecosystem	Related authorities	(i) (iv)
Requesting consumers, investors, and businesses to cooperate in addressing digital asset risks faced by them and maximize the effect	Related authorities	(ii)
Sharing of data on consumer complaints regarding digital assets	Related authorities	(ii)
Awareness-raising activities for consumers on risks of digital assets and fraudulent acts	Financial Literacy and Education Commission	(iv)

(i) Laws and regulations/rules, (ii) system establishment/enforcement, (iii) accounting/tax systems, (iv) public relations/information provision, and (v) Issues to be considered. * Note that the categories are for reference purposes only and not exhaustive.

2. Promotion of access to safe and affordable financial services		
In the U.S., about 7 million people do not have bank accounts and about 24 million people rely on costly non-bank services. It is necessary to develop financial services that are safe, reliable, affordable, and easy to use for anyone. Some digital assets may be able to realize faster payment and provide financial services in an easier-to-use manner. However, in order to provide true benefits to consumers who have not received sufficient services and avoid predatory financial practices, the following initiatives would be necessary:		
Encouraging introduction of immediate payment systems such as FedNow (support for development and use of innovative technologies by payment business operators: including use of immediate payment systems for their own transactions from the perspective of distribution of payments by the government to consumers in cases of disasters, emergencies, and otherwise)	Related authorities	(ii) (v)
Recommendations to authorities to create a federal government framework to regulate non-bank payment business operators	Related authorities	(i) (v)
Initiatives toward improving the efficiency of cross-border payment (pursuing a new multilateral platform which integrates immediate payment systems while working to align it with such matters as global payment practices and regulations)	Related authorities	(v)
Support for research in the fields of technologies and social technologies as well as the field of behavioral economics (to ensure that the digital asset ecosystem is designed in a manner that is easy to use, comprehensive, fair, and accessible to anyone)	National Science Foundation	(v)
3. Initiatives toward financial stability		
Ties between digital assets and core financial systems are becoming stronger, and a route is arising that will spill over into disruption. Stablecoins, in particular, may cause destructive disruption without appropriate regulations. Signs of instability have emerged in the collapse of stablecoin TerraUSD in May 2022 and its insolvency, in which about 600 billion dollars were lost after its collapse. The Financial Stability Oversight Council (FSOC) plans to announce additional recommendations on the promotion of financial stability which take the risks of digital assets into consideration in October 2022 (the announcement was already made on October 3, 2022). Additionally, the following measures are planned to be taken:		
Strengthening the ability to identify and mitigate cyber vulnerabilities of financial institutions (through efforts such as information sharing and promotion of a wide variety of data sets and analysis tools)	Department of the Treasury	(ii)

Identification, tracing, and analysis of new strategic risks related to the digital asset market	Department of the Treasury and related authorities	(v)
Cooperation on risk identification with allied nations of the U.S. through international organizations (such as the OECD and FSB)	Department of the Treasury	(ii) (v)
4. Promotion of responsible innovation		
Half of the 100 most valuable financial technology companies in the world (many of which are engaged in digital asset services) are located in the U.S. The U.S. government has played an important role in promoting responsible innovation of the private sector. The U.S. government plans to take the following measures from the perspective of providing support for cutting-edge research, strengthening the international competitiveness of companies, providing compliance support, and cooperating in efforts to mitigate negative and harmful side effects caused by technology innovations.		
Formulation of the “Digital Asset R&D Agendas” and commencement of basic research on matters such as next-generation cryptology, transaction programmability, cybersecurity, privacy protection, and mitigation of an impact of digital assets on the environment	Office of Science and Technology Policy National Science Foundation	(v)
Support for research on creation of products from technology innovations that can be launched in markets	Office of Science and Technology Policy National Science Foundation	(v)
Support for research on social science and education to develop methods to provide information for, educate, and train diverse stakeholders on safe and responsible use of digital assets	National Science Foundation	(iv) (v)
Sharing of regulatory guidance and best practices and provision of technological support to innovative U.S. companies which develop new financial technologies, through such means as Tech Sprint and Innovation Hours	Department of the Treasury Financial regulatory authorities	(iv)
Considering to provide tools, resources, and expertise to conduct studies on the impact of digital assets on the environment and to reduce environmental damage	Department of Energy, Environmental Protection Agency, and related authorities	(iv) (v)
Establishment of permanent forums where federal government	Department of	(ii)

agencies, industries, academic societies, and the general public can exchange knowledge and ideas that are useful to federal government regulations and standards, adjustment activities, technological support and research support	Commerce	(iv)

5. Reinforcement of leadership in the global financial system and competitiveness		
The following measures are planned to be taken to reinforce U.S. leadership in the global digital asset market:		
Planning to provide views of the U.S. on digital assets by making use of its positions in international organizations	Related authorities	(iv)
Maintaining and enhancing its leading role in initiatives related to digital assets in international organizations (such as the G7, G20, OECD, FSB, and FATF) (promotion of standards that reflect values such as data privacy, free and efficient markets, financial stability, consumer protection, strong law enforcement, and environmental sustainability)	Related authorities	(iv) (v)
Strengthening of cooperation and support with partner institutions of other countries through global enforcement agencies (e.g., the Egmont Group), bilateral information sharing, and capacity development	Department of State, Department of Justice Other enforcement agencies	(ii)
Technological support for developing countries (building of infrastructure and services for digital assets)	Department of State, Department of the Treasury, Agency for International Development, and others	(v)
Support for U.S. cutting-edge companies related to financial technologies and digital assets to create opportunity for launching their products in markets across the world	Department of Commerce	
6. Measures against illicit finance		
The U.S. has played a leading role in applying the AML/CFT framework to the digital asset ecosystem. However, digital assets (some of them are under disguised names which can be transferred without intervention of financial intermediaries) have been abused for unlawful money laundering, fund-raising for terrorism and proliferation of weapons of mass destruction, and various other crimes. For example, digital assets have been used for crimes such as the use of ransomware by cybercriminals, sale of narcotics by drug-smuggling rings, and money laundering. The following measures are planned to be taken to more effectively prevent the illegal use of digital assets.		
Considering whether to urge the assembly to revise the Bank	President	(i)

Secrecy Act, the anti-tip-off act, and the act on unauthorized fund transfers and apply them to digital asset service providers, including digital asset exchanges and NFT platforms		(v)
Considering whether to urge the assembly to tighten penal provisions for unauthorized transfers of money to a level equivalent to those in other money laundering regulations and to allow the Department of Justice to prosecute in the jurisdictions of the victims of digital asset crimes	President	(v)
Assessment of illicit finance risks related to decentralized finance (deadline: February 2023) and evaluation of NFTs (July 2023)	Department of the Treasury	(v)
Addressing the abuse of digital assets by continuing efforts to detect and eliminate illegal actors (such as pursuit of responsibility for illegal acts of cybercriminals and other malicious actors and identification of nodes within the crypto asset ecosystem that pose risks to national security)	Related authorities	(ii)
Enhancement of dialog with the private sector (enhancing understanding of obligations related to digital assets and of illicit finance risks among companies, information sharing, recommendation to use new technologies to comply with obligations)	Department of the Treasury	
7. Development of U.S. central bank digital currencies		

[Reference 8] Europe: Proposal for crypto assets market regulation (Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets (MiCA)), October 5, 2022 * Adopted by the Council of the European Union and submitted to the European Parliament

Basic views	
Potential of crypto assets	・ Crypto assets are digital representations of value or rights that have the potential to bring significant benefits to both market participants and retail holders. ・ Representation of value also includes external, non-intrinsic value attributed to a crypto asset by involved parties or market participants, meaning the value can be subjective and can be attributed only to the interest of someone purchasing the crypto asset. ・ By streamlining capital-raising processes and enhancing competition, offers of crypto assets can allow for an innovative and inclusive way of financing, including for small and medium-sized enterprises (SMEs). ・ When used as a means of payment, payment tokens can present opportunities in terms of cheaper, faster, and more efficient payments, particularly on a cross-border basis, by limiting the number of intermediaries. ・ It is expected that many applications of distributed ledger technology, including blockchain technology, that have not yet been fully studied will go on to create new types of business activities and business models which, together with the crypto asset sector itself, will lead to economic growth and new employment opportunities for EU citizens.
Necessity of the regulation	・ There are no rules, other than AML rules, for services related to these unregulated crypto assets, including for the operation of trading platforms for crypto assets, the service of exchanging crypto assets for funds or other crypto assets, or the custody of crypto assets. The lack of such rules leaves holders of crypto assets exposed to risks, in particular in areas not covered by consumer protection rules. The lack of such rules can also lead to substantial risks to the soundness of the market, including market manipulation, and financial crime. ・ The lack of an overall EU framework for crypto assets: ➢ can lead to a lack of users' confidence in crypto assets, which could significantly hinder the development of a market in those assets and can lead to missed opportunities in terms of innovative digital services, alternative payment instruments or new funding sources for EU

	companies; ➢ companies using crypto assets would have no legal certainty on how their crypto assets would be treated in the different EU Member States, which would undermine their efforts to use crypto assets for digital innovation; and ➢ could also lead to regulatory fragmentation, which would distort competition in the single market, make it more difficult for crypto asset service providers to scale up their activities on a cross-border basis, and would give rise to regulatory arbitrage.
Purpose of the regulation	・ To address the fragmentation of the legal framework applying to offerors of crypto assets, persons seeking admission to trading of crypto assets, issuers of asset-referenced tokens and e-money tokens and crypto asset service providers, and to ensure the proper functioning of crypto asset markets while ensuring protection of holders of crypto assets and clients of crypto asset service providers.
Definition	
・ **Crypto asset**: a digital representation of a value or a right which may be transferred and stored electronically, using distributed ledger technology or similar technology (categorized into the following three sub-categories): ① **E-money token**: a type of crypto asset that purports to maintain a stable value by referencing the value of one fiat currency; ② **Asset-referenced token**: a type of crypto asset that is not an e-money token and that purports to maintain a stable value by referencing any other value or right or a combination thereof, including one or more fiat currencies; and ③ **Utility token and other similar tokens**: a type of crypto asset which is only intended to provide access to goods or a service supplied by the issuer of that token. ・ **Crypto asset service provider**: Legal person or other business entity whose occupation or business is the provision of one or more crypto asset services to third parties on a professional basis.	
Subject of the regulation	
・ The regulation applies to natural and legal persons and other business entities that are engaged in the issuance, offer to the public, and admission to trading of crypto assets, or that provide services related to crypto assets in the EU. ・ NFTs are not subject to the regulation as they do not constitute crypto assets (however, fractional NFTs are considered to be regulated and therefore attention should be paid to applicability to NFTs).	

・ The proposal requests that the ESMA publish guidelines to clarify how to distinguish crypto assets which are subject to the regulation and financial instruments which are not.	
Details of the regulation	
Overview	・ Transparency and disclosure requirements for the issuance, offering to the public, and admission to trading of crypto assets on a trading platform for crypto assets ・ The authorization and supervision, operation, organization, and governance of crypto asset service providers, issuers of asset-referenced tokens, and issuers of e-money tokens; ・ Protection of holders of crypto assets in the issuance, offering to the public, and admission to trading ・ Protection of clients of crypto asset service providers ・ Measures to prevent insider dealing, unlawful disclosure of inside information, and market manipulation related to crypto assets in order to ensure the integrity of crypto asset markets
Major provisions for crypto assets other than e-money tokens and asset-referenced tokens	・ When offering crypto assets other than e-money tokens and asset-referenced tokens, the offeror must create a crypto asset white paper, notify the competent authority of the white paper, and publish the white paper. ・ A crypto asset white paper needs to contain the following information, among others: the issuer and related parties to the offering to the public, project to be implemented by the funds raised, details of the offering of crypto assets to the public, rights and obligations attached to the crypto assets, underlying technology, related risks, and information on principal environmental and climate related impact of the consensus mechanism. ・ The obligation to create a white paper does not apply when the conditions such as the following are met: the offering to the public is less than 150 natural or legal persons per EU Member State; over a period of 12 months, the total consideration does not exceed 1 million euro; the offer of crypto assets is solely addressed to qualified investors, and the crypto assets can only be purchased and held by such qualified investors.
Major provisions for e-money tokens	・ Issuers of e-money tokens need to be authorized as a credit institution under the EU Directive or an e-money institution under the EC Directive. E-money tokens shall be deemed to be “electronic money” as defined in the EC Directive, and shall be subject to the operational requirements set out in the EC Directive unless otherwise stated in the regulation. ・ The issuer of e-money tokens must create a crypto asset white paper, notify

	the competent authority of the white paper, and publish the white paper. ・ Holders of e-money tokens shall be given the right to redeem their tokens at any moment and at par value.
Major provisions for asset-referenced tokens	・ Issuers of asset-referenced tokens should have a registered office in the EU. ・ They must have the authorization, in principle. However, the authorization requirement does not apply to cases where asset-referenced tokens are offered only to qualified investors or where the offering of asset-referenced tokens to the public is below a certain threshold. The issuers are still required to produce a crypto asset white paper. ・ Issuers of asset-referenced tokens should create and maintain a reserve of assets matching the risks reflected in their liability. ・ Issuers of asset-referenced tokens shall give holders the right to claim redemption of their asset-referenced tokens at any time and at par value.
Major provisions for crypto asset service providers	・ They must have a registered office within the EU and at least one of the directors shall reside in the EU. ・ To ensure consumer protection, crypto asset providers should comply with some prudent requirements, depending on the types of services they provide. ・ The crypto asset service providers must ensure that all held crypto assets are unencumbered at all times. Those service providers should also be held liable for any damage resulting from an incident, including an incident resulting from a cyberattack, theft, or any malfunctions.