# Report of FSA's Joint Research on Analyzing Decentralized Financial System using On-Chain and Off-Chain Data

June 2023

QUNIE Corporation

# Purpose and Background of the Research

- In a decentralized financial system, many issues have been pointed out from the viewpoints of user protection, financial crime prevention, and financial stability, etc. In order to reap the fruits of technological innovation, it is essential to reduce these risks. In considering how to respond to various risks, risk assessment using objective and reliable data is considered important. However, as the FSB, FATF, and other organizations have pointed out in their reports, there is a lack of data necessary to understand the actual state of decentralized financial systems, including DeFi and P2P.

- Therefore, as part of the FSA's "International Joint Research on Blockchain" this research will conduct a survey on the actual status of distributed financial systems, including DeFi and P2P, using on-chain/off-chain data. In distributed financial systems, in addition to on-chain data such as transaction records on the blockchain, more in-depth data can be obtained by linking off-chain data such as IP addresses, web traffic, and sanctions-related information with blockchain addresses. We will conduct this research in order to understand the actual situation of such on-chain/off-chain data, including whether or not the data can be obtained, and to provide a useful perspective for considering future policy measures.

* Note that the addresses and transactions that can be analyzed with the blockchain analytics tools, etc. used in this research are only a small portion of the total, and not necessarily the data of the entire decentralized financial system. (See below for details).

# Acknowledgements and Disclaimer

**Acknowledgements**

- In preparing this report, we received useful advice and comments from Professor Naoyuki Iwashita of Kyoto University, Professor Kazue Sako of Waseda University, and Research Professor Shin'ichiro Matsuo of Georgetown University. We also received useful suggestions and advice from observers at the Digital Agency and the Bank of Japan, as well as from officials at the Financial Services Agency.
- However, any errors in the content regarding this report are attributed to the trustee, Qunie Corporation.

**Disclaimer**

- The contents of this report do not represent the official views of the JFSA.
- The contents in this report other than historical or current facts are forward-looking statements based on information available at the time of writing, and actual trends may vary due to a variety of uncertainties.

# Table of Contents

# Glossary

* Some of the terms in this report do not necessarily have fixed definitions, and there are also differences in definitions among blockchain analytics tool companies. Note that these terms are specified based on the definitions of the blockchain analytics tools employed in this report.

| Terminology | Definition |
|---|---|
| AML/CFT | Anti Money Laundering and Combating the Financing of Terrorism |
| DeFi | Decentralized Finance: Financial services provided through the use of smart contracts |
| DEX | Decentralized Exchange (a type of DeFi) |
| EOA | Externally Owned Account: Accounts on the Ethereum blockchain that are managed with a private key and can send and receive native tokens and other tokens and deploy and execute smart contracts |
| FATF | Financial Action Task Force on Money Laundering |
| FSB | Financial Stability Board |
| KYC | Know Your Customer: Customer Identification Program |
| P2P | Peer to Peer (Transaction): Transactions using unhosted wallets (for the purposes of this report, transactions between unhosted wallets) |
| TVL | Total Value Locked: Total crypto assets deposited with DeFi (locked in smart contracts) |
| VASP | Virtual Asset Service Provider: Providers of crypto asset exchanges, custodial (i.e. hosted) wallets, etc. |

# Glossary

| Terminology | Definition |
|---|---|
| On-chain data | • Data that can be obtained on the blockchain (addresses, transaction history, balances, and other smart contract status) |
| Off-chain data | • Data other than on-chain data<br>*In this report, layer 2 of the Ethereum blockchain (e.g., Arbitrum) is considered off-chain data. |
| BC Explorer | • For the purposes of this report, this refers to blockchain data analysis sites that are publicly available on websites (Etherscan, Dune Analytics, etc.) |
| Crypto asset-related databases | • For the purposes of this report, refers to crypto asset market information sites published on websites (CoinGecko, CoinMarketCap, etc.) |
| Blockchain analytics tools | • Analytics tools provided by blockchain analytics companies<br>• On-chain data can be queried and searched, information such as category and account names for some addresses identified by blockchain analytics companies, and transactions for high-risk addresses. |
| High Risk address | • For the purposes of this report, certain blockchain analytics companies calculate risk values on a scale of 100, based on the following information, with a score of 80 or higher being a "high-risk address"<br>➢ Addresses used for fraud and hacking<br>➢ Addresses posted on public sanctions lists<br>➢ Information from other blockchain analysis company<br>➢ Research information inside the blockchain company<br>➢ Information from Open Source Intel (OSINT) |
| High Risk Transaction | • Transactions where the senders or recipients of the transaction, or both, are high-risk addresses |
| Smart Contract | • A program that is written to the blockchain and defines rules that are automatically executed when a function is invoked through a transaction |

# Glossary

| Terminology | Definition |
|---|---|
| Token Contract | • Smart contracts that manage the amount of tokens (USDC/USDT, etc.) issued, owners, balances, etc. that comply with ERC-20 standards, etc.<br>• Owner, balance, etc. are updated as tokens are transferred*1 |
| Oracle Contracts | • Smart contracts that feed data to obtain off-chain external data<br>• Used primarily as a price oracle to obtain external market prices and interest rates*2 |
| Contract Account | • Account for deployed smart contracts<br>• Smart contracts are executed in response to messages received from EOA and other contract accounts*3 |
| Transaction | • Digitized and signed actions initiated by EOA<br>• In Ethereum, transfer tokens, deploy smart contracts, or invoke smart contract functions*4 |
| Block | • Data containing the hash (cryptographic digest) and transaction of one previous block in the blockchain<br>• Blocks are generated by a randomly selected validator on the Ethereum blockchain*5 |
| Bridge | • Also called a cross-chain bridge, a generic term for functions and services that provide a way to interconnect different blockchains and transmit tokens and other items.<br>• When the tokens to be sent between different blockchains are different, the tokens of the source blockchain are generally locked (frozen) in the bridge and exchanged for the tokens of the destination blockchain*6. |
| Hosted Wallet | • Wallet provided by VASP and others<br>• Users entrust the management of their private keys to VASPs, etc. (wallet administrators), and VASPs can intervene and execute transfer transactions, etc. of users' cryptographic assets. |
| Unhosted Wallet | • Wallets in which users directly manage their private keys without going through a VASP, etc. Users can generally execute cryptographic asset transfer transactions, etc. directly. |

*1: Ethereum.org ERC-20 TOKEN STANDARD https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
*2: Ethereum.org ORACLES https://ethereum.org/en/developers/docs/oracles/
*3: Ethereum.org ETHEREUM ACCOUNTS https://ethereum.org/en/developers/docs/accounts/
*4: Ethereum.org TRANSACTIONS https://ethereum.org/en/developers/docs/transactions/
*5: Ethereum.org BLOCKS https://ethereum.org/en/developers/docs/blocks/
*6: Ethereum.org BRIDGES https://ethereum.org/en/developers/docs/bridges/

# Chapter 1: The Need for Data Analysis in Distributed Financial Systems

# Chapter 1: The Need for Data Analysis in Decentralized Financial Systems

- In this chapter, we will organize the types of data needed to understand the actual state of decentralized financial systems from the perspective of financial authorities and the possibility of obtaining such data. In particular, the FSB report and the FATF report on data gaps will be used as a starting point.
- This chapter is organized as follows
  - Section 1-1, Explain the factors contributing to the data gaps identified in the FSB report and examples of available/unavailable data and additional data to be obtained.
  - Section 1-2, Explain the results of the investigation of P2P transactions by blockchain analytics companies as pointed out in the FATF report, and examples of red flags indicators in the identification of AML/CFT crypto asset related data.

# 1-1. Data Gap Issues Identified in the FSB Reports

(1) FSB report issues

- In a report (published in February 2023) pointing out the financial stability risks of DeFi and other issues, the report points out the problem of lack of transparency and consistency of data in the crypto asset market, including DeFi. (see table below)
- In the future, they will work with Standard Setting Bodies (SSBs) and regulators to consider approaches to fill data gaps to measure and monitor DeFi interconnections.

Table 1-1-1 Data Gap Factors in the FSB Report

| Data gaps factor | Details |
|---|---|
| **Difficulty in aggregating and analyzing the vast amount of data available on a distributed ledger** | • While data from public blockchains is transparent and immutable in some respects, it is generally difficult to collect and analyze due to its sheer volume. |
| **Information on the public ledger is anonymous** | • While transaction data at the wallet level is accessible, the lack of data on the identity of the wallet owner makes vulnerability assessment very difficult.<br>• Various privacy-enhancing technologies (wallet mixers/tumblers/anonymity-enhancing crypto assets, etc.) exist that can obscure the transparency of transactions by certain users. |
| **A lot of off-chain data** | • The large amount of off-chain data in the crypto asset market, including DeFi, makes it difficult to get a picture of overall market activity from on-chain data alone. |
| **No obligation to report consistent data in accordance with regulations** | • A portion of the crypto asset ecosystem is currently outside of, or not in compliance with, the regulatory framework and is therefore not obligated to produce and report consistent and reliable data, or is not in compliance with its obligations. |
| **Possibility of data manipulation by data providers** | • Some data providers may be incentivized to manipulate data to make their respective platforms appear more important and attract additional transaction volume or investment. Market incentives for trading and lending platforms, coupled with participants who deviate from or act without compliance with the existing regulatory framework, increase the risk of market manipulation and data falsification. |

Source: FSB, The Financial Stability Risks of Decentralized Finance, February 2023, https://www.fsb.org/2023/02/the-financial-stability-risks-of- decentralised-finance/

# 1-1. Data Gap Issues Identified in the FSB Reports

(2) FSB report issues (example data)

- Examples of available/unavailable data to be obtained, as noted by the FSB, are as follows
- Based on these points, this research identifies the data sets that are desirable to obtain, and verifies the availability and reliability of each data set using blockchain analytics tools.

Table 1-1-2-1 Data Gaps for Unbacked crypto-assets

| Transmission Channels | Available Metrics | Data Gaps |
|---|---|---|
| **Wealth Effects** | • Market capitalization of crypto-assets<br>• Trading volumes<br>• Realized volatility and gamma<br>• Geographical adoption | • Share of households invested in crypto-assets<br>• Share of assets relative to household wealth<br>• Demographic skew among household's holdings<br>• Owners of unbacked crypto-assets |
| **Confidence Effects** | • Share of retail ownership of crypto-assets<br>• Number of clients in infrastructures that provide access to crypto-assets (e.g. trading platforms, wallet providers) | • Volume of crypto-asset fraud |
| **Financial Sector Exposure** | • Share of institutional ownership of crypto-assets<br>• Share of assets invested in crypto-assets<br>• Number of large financial service providers offering crypto-asset services<br>• Volume of crypto-asset derivatives market<br>• Open interest of crypto-asset derivative contracts<br>• Correlations of crypto-assets with other asset classes<br>• Share of transaction volume by transaction size | • AUM and share of holdings of funds that offer exposure to crypto-assets (by asset type e.g. spot, derivative, eco-system and investor type)<br>• Bank sector exposure (absolute vs hedged; change in open interest)<br>• Reporting by financial institutions on crypto-assets held and serviced |
| **Use in Payments and Settlements** | • Prices and delta (over one week, 1m, 3m, 6m, 1y)<br>• Trading volumes (absolute vs. average)<br>• Number of large payment service providers supporting crypto-assets<br>• Market share of major crypto-asset exchanges | • Number and value of transactions<br>– Jurisdiction of the payers and payees<br>– Type of transactions (e.g. remittances, ecommerce, trading)<br>• Types of crypto-assets employed<br>• Acceptance as legal tender |

Source: FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to- financial-stability-from-crypto-assets/

# 1-1. Data Gap Issues Identified in the FSB Reports

(2) FSB report issues (example data)

Table 1-1-2-2 Data issues for stablecoins

| Transmission Channels | Available Metrics | Data Gaps | Data to be added (as noted by experts) |
|---|---|---|---|
| **Wealth Effects** | • Market capitalization of stablecoins<br>• Trading volumes<br>• Realized volatility | • Owners of stablecoins | • Business relationship between VASP and issuers of stablecoins |
| **Confidence Effects** | • Share of retail ownership of stablecoins<br>• Number of clients in infrastructures that provide access to stablecoins (e.g. trading platforms, wallet providers) | • Volume of crypto-asset fraud | • Addresses to be frozen<br>• Total amount subject to be frozen |
| **Financial Sector Exposure** | • Share of institutional ownership of stablecoins<br>• Share of assets invested in stablecoins<br>• Number of large financial service providers offering stablecoin services<br>• Size of stablecoin market relative to US prime money market funds | • Amounts and share of holdings of ETFs that offer exposure to stablecoins (by investor type)<br>• Profit and loss exposures<br>• Reserve assets invested in regulated markets<br>• Liquidity of reserve assets<br>• Granular and robust data on composition of stablecoins reserve assets<br>• Reporting by financial institutions on crypto-assets held and serviced | • Actual crypto asset transactions by institutional investors and financial institutions (e.g., types of crypto assets/stablecoins preferred by large users) |
| **Use in Payments and Settlements** | • Prices<br>• Trading volumes<br>• Number of large payment service providers supporting stablecoins | • Number and value of transactions<br>• Jurisdiction of the payers and payees<br>• Type of transactions (e.g. remittances, e-commerce, trading)<br>• Usage in crypto-asset trading platforms, by stablecoin<br>• Breakdown of uses of stablecoins | - |

Source: FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to- financial-stability-from-crypto-assets/

# 1-1. Data Gap Issues Identified in the FSB Reports

(2) FSB report issues (example data)

Table 1-1-2-3 Data issues for DeFi (1/2)

| Transmission Channels | Available Metrics | Data Gaps | Data to be added (as noted by experts) |
|---|---|---|---|
| **Wealth Effects** | • Total value locked-in, gross, adjusted and net; realized volatility<br>• Transaction volume of DeFi's Exchange (DEX)<br>• Wallet growth<br>• Market capitalization and transaction volume of governance tokens;<br>• Transaction volume in DeFi lending<br>• Lending rate in DeFi Lending<br>• Utilization rate of liquidity pool of DeFi Lending and Exchange<br>• DeFi yield and return | • Share of retail vs institutional participation<br>• Number of dApps on a blockchain<br>• Liquidity pools, DeFi stablecoins, derivatives (entities within the DeFi space, including types of financial institutions (specialized or traditional financial institutions) to understand linkages of DeFi with the rest of the financial system)<br>• Metrics to measure leverage<br>• Information on the governance tokens holders could be obtained from to see to what extent the governance is decentralized (e.g. if the ownership of governance tokens is concentrated, that entity could be considered the actual developer) | • TVL (TVL-based market share of major DeFi protocols)<br>• Market Capitalization of Stablecoin<br>• Degree of linkage between major DeFi (DEX-Lending, etc.)<br>• Total tokens locked in the cross-chain bridge<br>• Cross Chain Bridge's business relationship with VASP<br>• Oracle's market share in TVL and other measures<br>• Collateral ratios, leverage ratios, and actual rehypothecation according to collateral type for lending protocols<br>• Major remittance address from Treasury Protocol |
| **Confidence Effects** | • Number of clients in infrastructures that provide access to DeFi (e.g. trading platforms, wallet providers) | • Volume of crypto-asset fraud<br>• Share of transactions in unbacked crypto-assets vs. stablecoins | • Governance Token Concentration<br>• DeFi Protocol Concentration<br>• Total amount and number of DeFi-related hacking losses |

Source: FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to- financial-stability-from-crypto-assets/

# 1-1. Data Gap Issues Identified in the FSB Reports

(2) FSB report issues (example data)

Table 1-1-2-3 Data issues for DeFi (2/2)

| Transmission Channels | Available Metrics | Data Gaps | Data to be added (as noted by experts) |
|---|---|---|---|
| **Financial Sector Exposure** | • Share of institutional ownership of crypto-assets<br>• Share of assets invested in crypto-assets<br>• Number of large financial service providers offering crypto-asset services<br>• Volume of crypto-asset derivatives market<br>• Open interest of derivative contracts<br>• Correlations of crypto-assets with other asset classes<br>• Share of transaction volume by transaction size | • Amounts and share of holdings of ETFs that offer exposure to crypto-assets by investor type | • Amount invested in traditional financial assets utilizing tokens locked to smart contracts as collateral |
| **Use in Payments and Settlements** | • Price of key players (DOT, UNI, LINK) and delta over one week, one month, three months, six months, one year and 7-day average volume; | • Number and value of transactions<br>• Breakdown of counterparties<br>– Jurisdiction of the payers and payees<br>– Type of transactions (e.g. remittances, ecommerce, trading) | - |

Source: FSB, Assessment of Risks to Financial Stability from Crypto-assets, February 2022, https://www.fsb.org/2022/02/assessment-of-risks-to- financial-stability-from-crypto-assets/

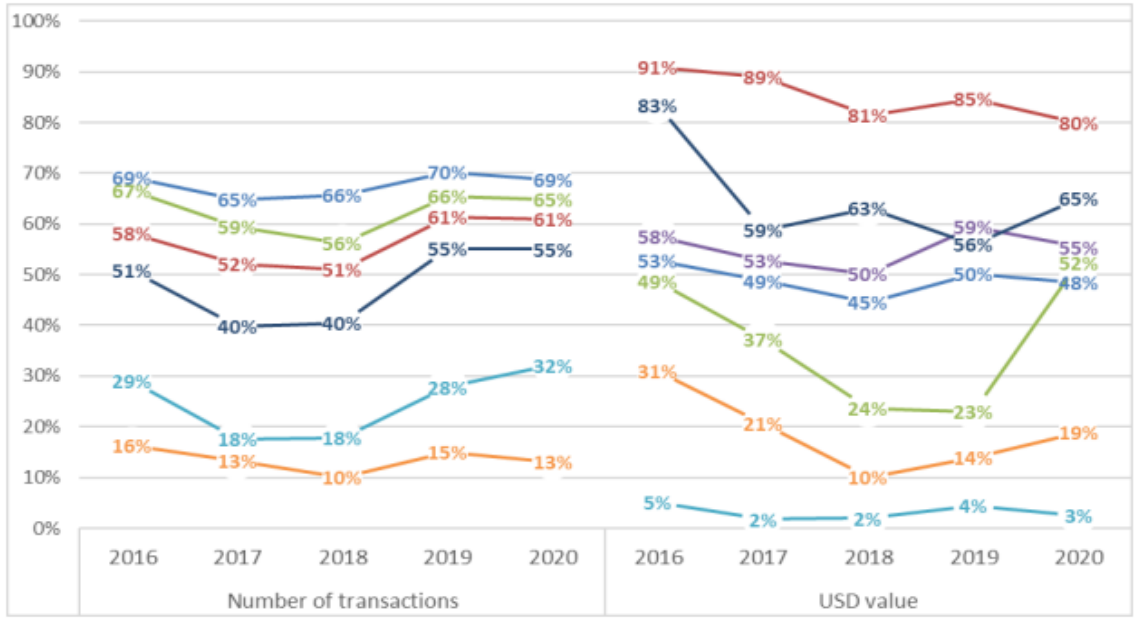
# 1-2. Data Gap Issues Identified in FATF Reports

(1) FATF report issues (P2P transactions)

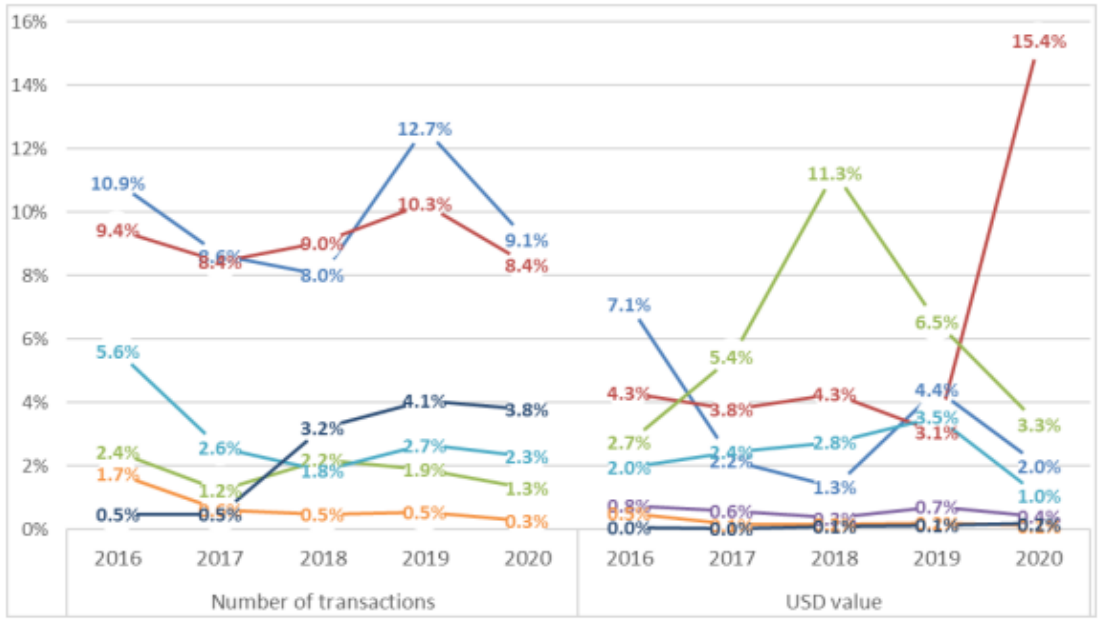
- The July 2021 FATF report reported that the findings of several blockchain analytics company on the actual status of P2P transactions (e.g., the percentage of total P2P transactions) showed a wide variation in results.
- Regarding the percentage of bitcoin transactions that occurred without VASP between 2016 and 2020, four companies analyzed 40% to 70% in terms of number of transactions, while two companies analyzed 10%~32%. In addition, for the value of transactions (in US dollars), a large variation exists in the company's analysis, ranging from 2% to 91% (Graph 2).
- A variation of 0.3% to 12.7% in terms of number of transactions and 0% to 15.4% in terms of transaction value (USD) exists for the percentage of fraudulent bitcoin transactions identified between 2016 and 2020 (Graph 3).

Fig. 1-2-1 Example of FATF report's findings on P2P transactions and illicit transactions

**Graph 2: Proportion of bitcoin transactions which occur without a VASP between 2016-2020 (left: number of transactions;12 right: USD value13)**




**Graph 3: Proportion of identified illicit bitcoin transactions between 2016-2020 (left: number of transactions[15]; right: USD value[16])**




Source: FATF, Second 12-Month Review of the Revised FATF Standards on Virtual Assets/VASPs, July 2021 https://www.fatf-gafi.org/en/publications/ Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html

# 1-2. Data Gap Issues Identified in FATF Reports

(2) FATF report issues (AML/CFT related)

- The September 2020 FATF report noted that not only can money launderers, terrorist financiers, and other criminals obtain, move, and store assets digitally outside of the regulated financial system, but also that it is difficult for reporting entities to identify suspicious activity in a timely manner, obfuscating the source and destination of funds The report also points out that it is difficult for reporting entities to identify suspicious activity in a timely manner.
- In light of the above points, we have published a report on ML/TF red flags related to crypto assets to assist reporting entities, including VASPs, in identifying and reporting potential ML and TF activities related to crypto assets.

Table 1-2-2 Red Flag Indicators

| Red flag Indicators | Use Case Examples |
|---|---|
| **Size and frequency of transactions** | • Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.<br>• Making multiple high-value transactions in short succession, such as within a 24-hour period, etc. |
| **Transaction Patterns** | • A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.<br>• Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account, etc. |
| **Anonymity** | • VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.<br>• Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports, etc. |
| **Senders or Recipients** | • A customer's VA address appears on public forums associated with illegal activity.<br>• A customer is known via publicly available information to law enforcement due to previous criminal association, etc. |
| **Source of Funds or Wealth** | • Transacting with VA addresses that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.<br>• VA transactions originating from or destined to online gambling services, etc. |
| **Geographical Risks** | • Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.<br>• Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls. |

Source: FATF, Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020 https://www.fatf-gafi.org/en/ publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

# Chapter 2: On-Chain/Off-Chain Data Mapping

# Chapter 2: On-Chain/Off-Chain Data Mapping

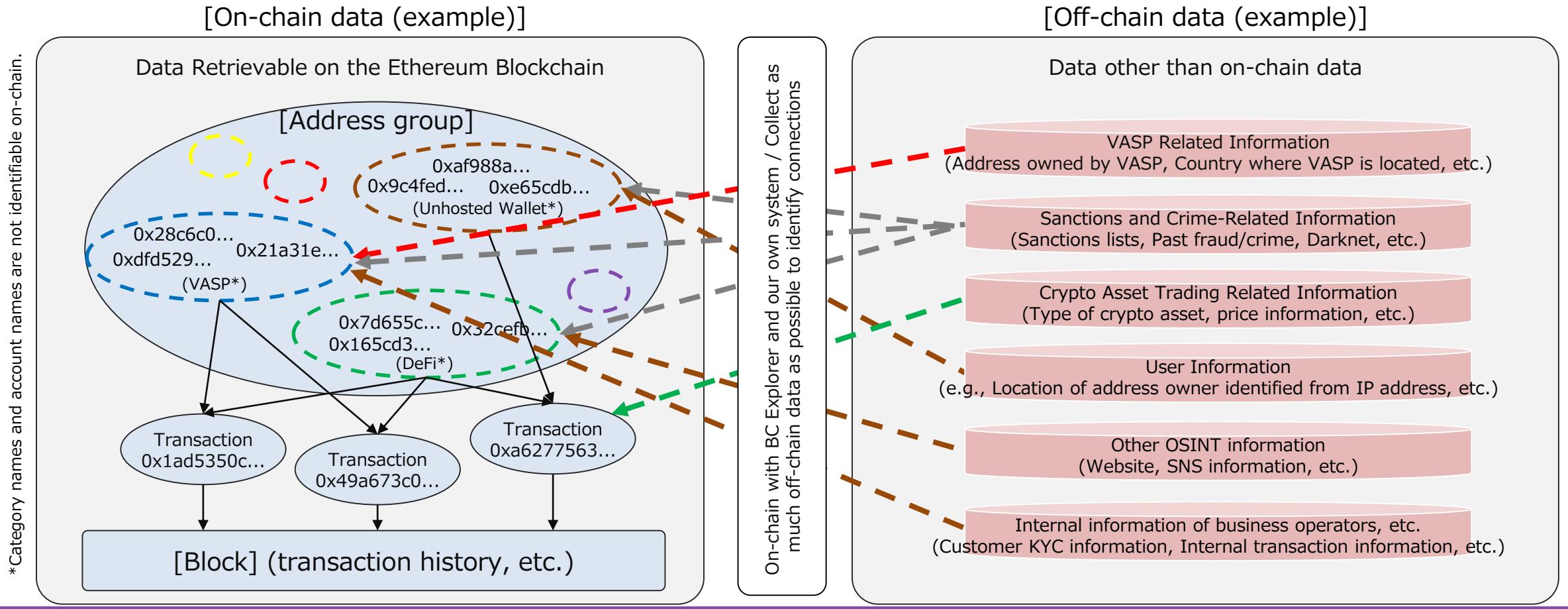
- In order to analyze data in a decentralized financial system, there is a limit to using only a random list of numbers and letters, such as wallet addresses and transaction IDs, which can be obtained on-chain. It is necessary to link these on-chain data with data outside the blockchain, such as wallet owners (off-chain data), to understand the actual status of transaction relationships, etc. Therefore, this chapter attempts to provide an overview of on-chain/off-chain data, organize its components, and map both types of data.
- Specifically, we organized the elements and connections between on-chain data and other off-chain data that can be obtained on the Ethereum blockchain. Based on this, we mapped the overall picture of on-chain/off-chain data.
- This chapter is organized as follows
  - Section 2-1, Describes the components of on-chain/off-chain data.
  - Section 2-2, Describes the mapping of on-chain/off-chain data.

# 2-1. Elements of On-chain/Off-chain Data

(1) On-chain/off-chain data connections

- Blockchain analytics company typically utilize open source and proprietary tools and know-how to collect both on-chain and off-chain data, group related addresses, label addresses (e.g., assigning a VASP's account name to a set of addresses managed by a particular VASP), and calculate address risk scores. ), and calculate risk scores for addresses.
- Below is an image showing some of the various data that blockchain analytics tool companies are collecting and the connections between them.

Figure 2-1-1 Main connections between on-chain and off-chain data (image)



# 2-1. Elements of On-chain/Off-chain Data

(2) Elements of off-chain data

- Possible elements of off-chain data tied to on-chain data include the following. (On-chain data is defined in the glossary, so the explanation is omitted.)

  * This page does not discuss the availability of each piece of data, and the table is a sampling of the major on-chain data that are generally believed to exist.

- The relationship between the respective off-chain and on-chain data is shown in the mapping diagram in the next section.

Table 2-1-2 Major Components of Off-Chain Data (1/2)

| Classification | Data Element | | Data Contents |
|---|---|---|---|
| Off-chain data | Token Transaction Price | | • Transaction prices of various crypto assets, etc. offered by VASPs, etc. |
| | | Hosted Wallet | • Users' IP addresses, KYC information (name, address, date of birth, credit card information, etc.), transaction history, wallet private keys, web traffic data, etc. |
| | | Unhosted Wallet | • User information for wallets such as Metamask, including the user's IP address, wallet private key, and web traffic data |
| | | DeFi User Interface | • User information such as IP addresses of users via interfaces, web traffic data, etc. as user information for DeFi, etc. |
| | Transaction information outside the blockchain | | • Information on transactions outside the blockchain, such as transfers of crypto assets between customers by rebooking within the VASP, etc. |
| | Governance Voter Information | | • Information related to governance voting in DeFi, DAO, etc., including the identity of the voter (e.g., user name on Discord, etc.) |
| | Infrastructure service user information such as nodes and APIs | | • Information on infrastructure service users who use Ethereum nodes and Ethereum blockchain API services, including users' IP addresses, KYC information (name, address, date of birth, credit card information, etc.), and number of API calls |
| | Github source code, parameters, etc. | | • Source code, parameters, etc. of smart contracts posted on Github (a software development platform for storing and publishing programs, etc.), etc. |
| | Information on assets backing stablecoin issuances | | • Name of the financial institution that manages the bank deposits, government bonds, and other assets backing stablecoin issuances, as well as the type and amount of assets. |

# 2-1. Elements of On-chain/Off-chain Data

(2) Elements of off-chain data

Table 2-1-2 Major Components of Off-Chain Data (2/2)

| Classification | Data Element | |
|---|---|---|
| Off-chain data | Validator Information | • Validator information, such as IP address of the validator node, secret key, etc. |
| | Staking Information | • Validator staking information, such as the investor and amount of money that will be used for staking services |
| | Layer 2 Transaction Information | • Transaction information executed at Layer 2, such as the user's address, sending address, amount transferred, etc.<br>(Layer 2 is defined as off-chain data in this research) |
| | Bridge node information | • Information on the node operated by the bridge administrator, such as IP address and secret key |
| | Token information locked on the bridge | • Information about the tokens locked on the bridge, including the type and amount of tokens locked |

# 2-1. Elements of On-chain/Off-chain Data

(3) Connection points for on-chain/off-chain data

- Nodal points such as wallets and interfaces generally exist between on-chain and off-chain data. The table shows the major connection points.
- The relationship between each connection point and on-chain/off-chain data is shown in the mapping diagram below.

Table 2-1-3 On-chain/off-chain connection points

| Connection point | | Description (specific examples of connections) |
|---|---|---|
| External Oracle | | • Oracle provider provides crypto asset prices, etc. provided by VASP to protocols in the blockchain (DeFi, etc.) |
| Wallet | Hosted Wallet | • VASP (hosted wallet provider) manages customer information and private keys, and customers instruct the VASP to transfer tokens from the wallet. |
| | Unhosted Wallet | • Using a wallet provided by software companies (wallet provider), the user directly manages the private key to transfer tokens, etc. |
| User Interface | | • DeFi and others operate user interfaces such as websites and smartphone applications, and users use the services directly. |
| Node | Smart contract developer node | • Smart contract developer deploys smart contract on blockchain based on source code on GitHub (may also be deployed from wallet) |
| | Stablecoin Operator Node | • Stablecoin operator issues and burns stablecoins with administrative authority. |
| | Validator Nodes | • Validators participate in the blockchain consensus by depositing participation fees and registering clients to generate and approve blocks |
| | Layer 2 operator node | • Layer 2 operator executes transactions on the Layer 2 blockchain and forwards the results to the Layer 1 main chain |
| | Bridge administrator node | • Bridge administrators send and verify tokens and other information that users exchange with each other between different blockchains. |

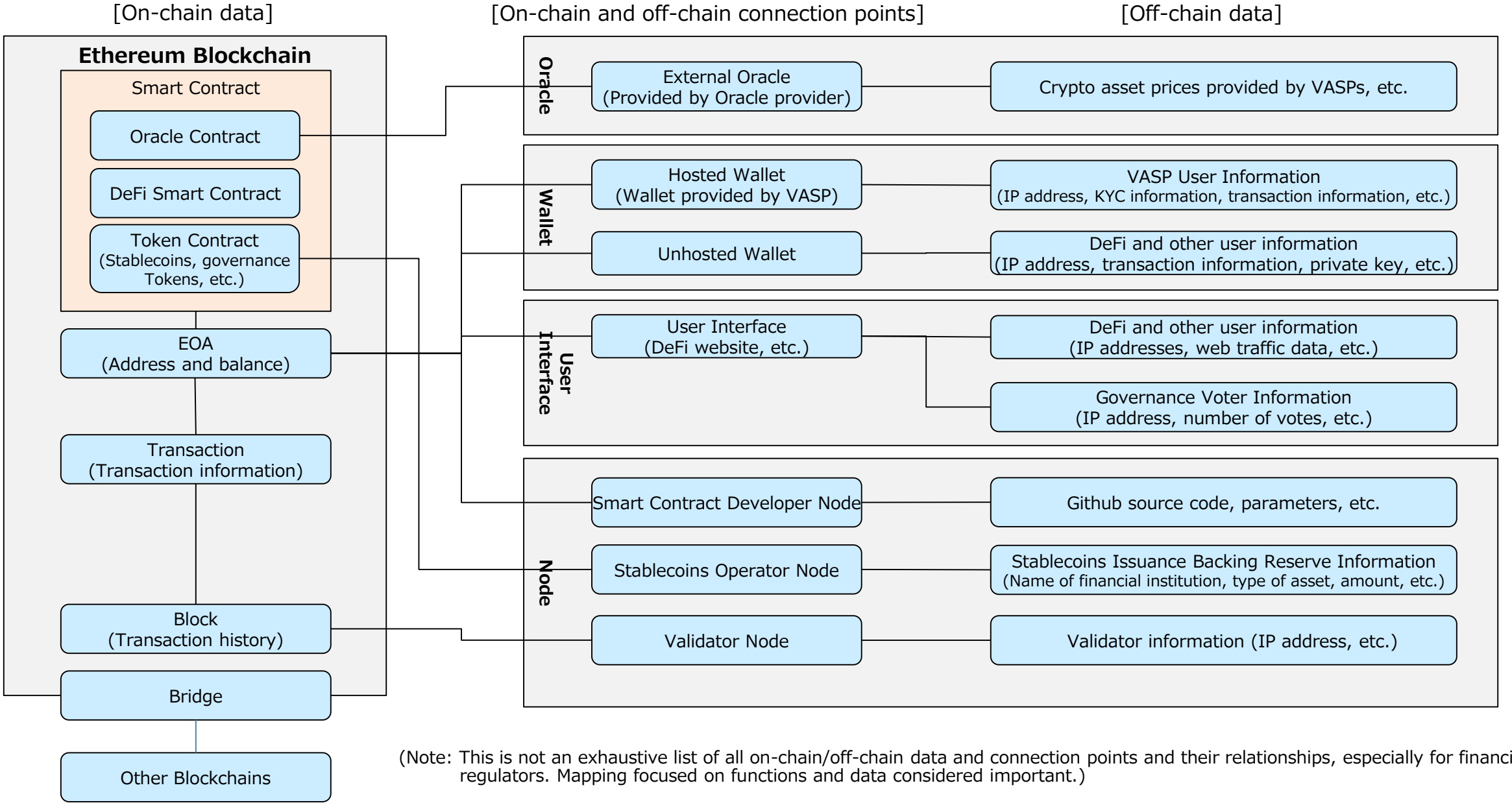
# 2-2. On-chain/Off-chain Data Mapping

(1) On-chain/off-chain data mapping

- We extracted and mapped the main components of the on-chain/off-chain data of the Ethereum blockchain and visualized the following three points.
  - Main components and overall classification of on-chain data, connection points, and off-chain data
  - Connection between on-chain data, connection points, and off-chain data
  - Manager of the off-chain data (organization or person who manages the off-chain data) *only in the detailed version

# 2-2. On-chain/Off-chain Data Mapping

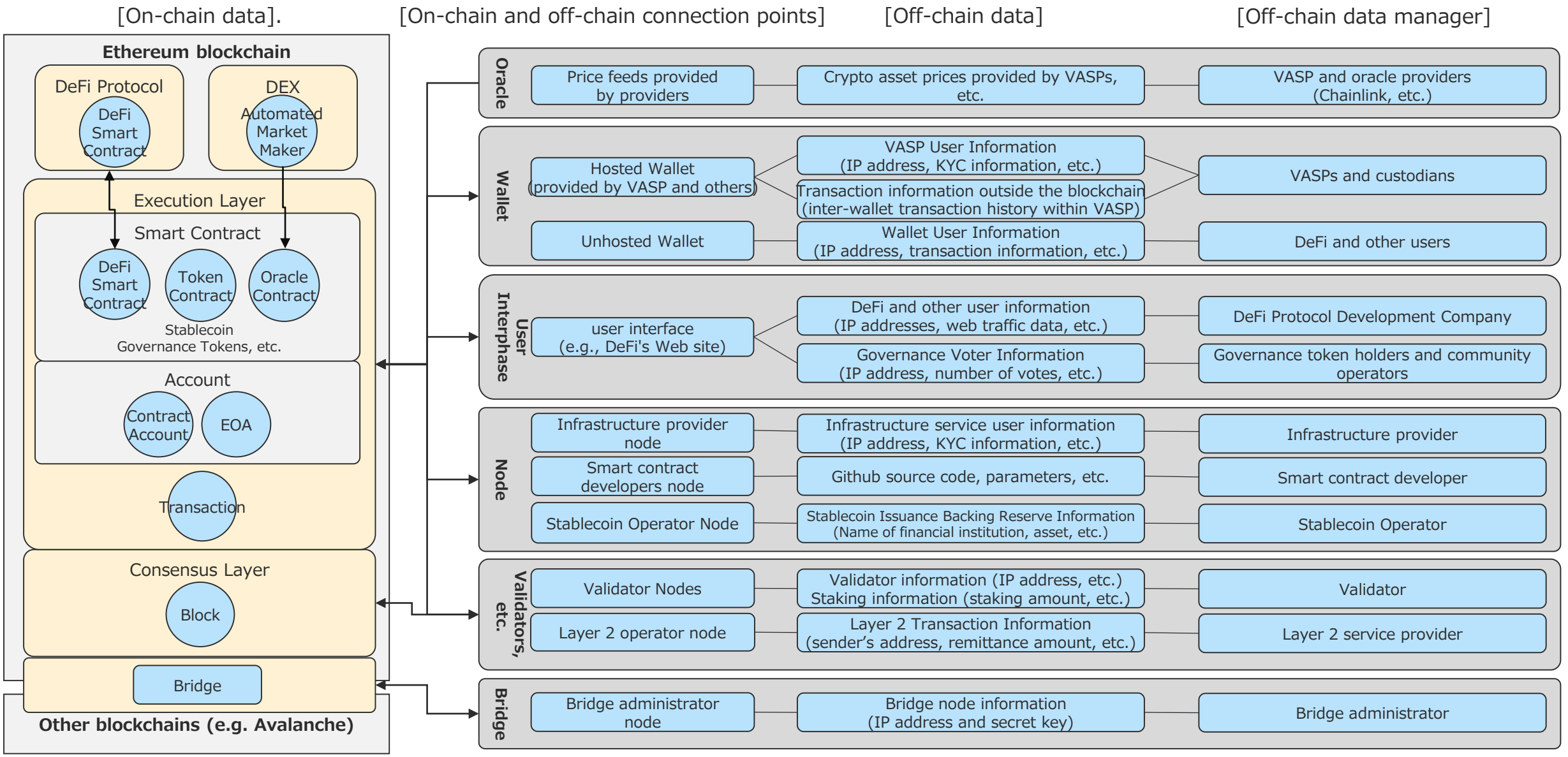
Figure 2-2-1 On-chain/off-chain data mapping (overview version)




(Note: This is not an exhaustive list of all on-chain/off-chain data and connection points and their relationships, especially for financial regulators. Mapping focused on functions and data considered important.)

# 2-2. On-chain/Off-chain Data Mapping

Figure 2-2-2 On-chain/off-chain data mapping (detailed version)



# Chapter 3: Survey and Examination of Data Necessary to Understand the Actual State of Decentralized Financial Systems

# Chapter 3: Survey and Examination of Data Necessary to Understand the Actual State of Decentralized Financial Systems

- Based on the organization of on-chain/off-chain data and connection points up to the previous chapter, this chapter details the data sources considered useful as sources of these data, the range of data sources utilized in the data analysis of this research, and the data survey methodology.
- This chapter is organized as follows
  - Section 3-1, Summarize the various data sources that are considered useful for understanding the actual state of decentralized financial systems, and then indicate the range of data sources actually utilized in this research.
  - Section 3-2, Provide an overview of the survey methodology used in the data analysis.
  - Section 3-3, Provide an overview of the blockchain analytics tools that were heavily used in this data analysis.

# 3-1. Various Data Sources and Scope of This Research

- As shown in the table, various data sources exist, but in addition to on-chain/off-chain differences, data reliability, availability, and accessibility (i.e., free of charge) vary widely. While understanding the characteristics of each type of data, it is necessary to analyze data according to regulatory objectives.
- In this research, we will utilize "BC (blockchain) Explorer," "cryptographic asset-related databases," and "blockchain analytics tool company (analytics tool researchers)," which may be able to obtain data of a different nature from the data available due to supervisory actions, etc., to conduct data analysis, etc.

Table 3-1 Various Data Sources and Scope of this Research

| Data Source | Businesses, etc. (Inside Information) | Businesses, etc. (Disclosure Information) | BC Explorer | Crypto Asset-Related Database | Blockchain Analysis Tool Company |
|---|---|---|---|---|---|
| **Summary** | Data obtained from reporting requests | Information legally disclosed by listed companies, etc. | Blockchain account and transaction-related data | Crypto asset prices and other data | Data obtained from blockchain analytics tools/researchers |
| **Public / Private** | Private | Public | Public | Public | Private |
| **On-chain/Off-chain** | Off-chain | Off-chain | On-chain | (Many are) Off-chain | Combination of on-chain and off-chain |
| **Data Reliability** | High | High | High | Medium (Many informations are on VASPs declaration basis) | Medium to low? |
| **VASP** | ○ | ○ | △ (Certain information is available regarding major VASPs) | ○ to △ (Some VASPs are difficult to obtain) | ○ to △ (Depends on the capability of the blockchain analytics tool companiy) |
| **(Unregistered) VASP** | × | × | △ to × | ○ to △ (Some VASPs are difficult to obtain) | ○ to △ (Depends on the capability of the blockchain analytics tool company) |
| **DeFi** | △ to x (May be obtained for DeFi regulated as VASP) | × (Some DeFi may voluntarily disclose information) | △ (Data on contract addresses, etc. can be obtained) | △ (Data on DEX, etc. can be obtained) | ○ to △ (Depends on the capability of the blockchain analytics tool company) |
| **Unhosted Wallet (including P2P)** | △ (VASP-Unhosted Wallet-related data may be available) | × | △ to x (Some unhosted wallets may be obtained) | × | △ (Depends on the capability of the blockchain analytics tool company, but is it accurate or not) |

Scope of this research

*Note that blockchain analytics tools vary in functionality and characteristics, and the range of data that can be obtained and the level of confidence in the data varies.

# 3-2. Survey Method

(1) Outline

- The data available from each of the data sources and the methodology of this research are as follows

Table 3-2-1 Data Sources and Survey Methods Utilized in this Research

| Data Source | | Data that can be obtained | Survey Methodology for this research |
|---|---|---|---|
| **BC (Blockchain) explorer** | | • Data such as blockchain addresses and transactions available from public Web sites<br>• Data such as category name (VASP, DeFi, etc.)/account name assigned to the address that identified the target | • Investigate data that can be obtained by referring to public Web sites<br>• Main survey targets<br>➢ Etherscan<br>➢ Dune Analytics, etc. |
| **Crypto asset-related databases** | | • Data on crypto asset prices, market price charts, market capitalization, and number of recent transactions available from public Web sites<br>• Transaction data, latest news, etc. on specific crypto assets, crypto asset traders, etc. | • Investigate data that can be obtained by referring to public Web sites<br>• Main survey targets<br>➢ CoinGecko<br>➢ Coinmarketcap |
| **Blockchain analytics company** | **Blockchain Analytics tools** | • Data that can be obtained from analytics tools provided by blockchain analytics company<br>(address holder category/account name, risk score based on sanctions and past criminal history, etc.) | • Investigate data that can be obtained from multiple blockchain analytics company tools<br>(Avoid risk of relying on data from one company) |
| | **Research by Experts** | • Data from research conducted by experts from blockchain analytics company<br>(e.g. data on complex conditions combining on-chain data with in-house databases, etc.) | • Outsource research to specific blockchain analytics company to obtain necessary data |

# 3-2. Survey Method

(2) Candidate data for analysis

- As noted in the table, the data considered to be obtainable differed by each method. On the other hand, based on the fact that much of the information that can be obtained from (1) BC Explorer is also incorporated into (3) and (4), etc., data analysis was conducted primarily using (2), (3) and (4).
- By contracting with multiple companies, the blockchain analytics tool attempted to reduce the risk of relying on data from one company (whose reliability is difficult for us to verify).

Table 3-2-2 Examples of data that can be obtained

| | | (1) BC Explorer | (2) Crypto-asset related database | (3) Blockchain analytics tools | (4) Research by experts |
|---|---|---|---|---|---|
| Main Features | | • Websites that allow users to search and query data in the blockchain<br>• Some major VASPs and DeFi can get the address from the account name | • Web site offering real-time market prices for crypto assets | • Analytical tools provided by blockchain companies<br>• Provides risk indication of specific entities, addresses, and alert detection of high-risk address transactions for investigative authorities, etc. | • In-depth research conducted by experts from blockchain analytics company using information from their own analytics tools and databases |
| Data Availability | On-chain data | • Block information (block number, number of transactions, etc.)<br>• Account information (address, balance by token, etc.)<br>• Transaction information (transaction time, number, etc.)<br>*Data can be obtained for each account/transaction (overall statistics cannot be obtained) | • Major DeFi TVL Token Issuance Volume<br>• Trading information on major decentralized exchanges (last 24 hours trading volume, number of token pairs/trade volume by pair, etc.) | • Account information (address, balance by token, etc.)<br>• Transaction information (last 24-hour trading volume, first/last trade date, trade date, number of trades, volume, etc.)<br>• Diagram display of account counterparties, etc. | • Aggregation of transactions based on complex search criteria (small transactions, multiple transfers to the same party in a short period of time, fraudulent address users, etc.)<br>• Anonymous service address<br>• Token freeze address, transaction volume, etc. |
| | Off-chain data | • Account names for some addresses (e.g. some VASPs and DeFi that publish addresses) | • List of token prices per VASP<br>• Token Price Trend Chart (From the 1st to the whole period)<br>• Chart of market capitalization of tokens<br>• Latest Crypto Asset News<br>• Overview of major tokens (founder, characteristics, etc.) | • Category name and account name of the identified address<br>• Risk value of an address<br>Risk values are self-determined by the blockchain analytics company<br>• Account Information (country licenses held, level of KYC enforcement, etc.) | • Aggregation of transactions by category and account<br>• Aggregate VASP information<br>• Number of hacking victims and amount of damage<br>• Aggregation of fraudulent addresses (sanctioned lists, fraud extortion, darknet, etc.)<br>• Number of VASP users, etc. |

# 3-3. Overview of Blockchain analytics tools

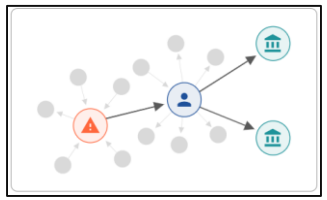
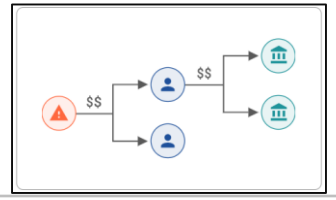
- Blockchain analytics tools are generally paid software provided by private companies that combine on-chain and off-chain data to identify category and account names and determine the risk score of the corresponding addresses using clustering techniques, etc. Blockchain analytics tools are mainly used by VASPs, institutional investors, investigative authorities, etc. for the purpose of detecting transactions with high-risk addresses and identifying account names of addresses under investigation (e.g., theft of cryptographic assets).
- The following table summarizes the data and other information provided by the analytics tools used in this study (note that the information obtained, its accuracy, and its scope vary depending on the tool).

Table 3-3 Overview of Blockchain analytics tools (1/2)

| Item | Data and services | Specifics | Remarks |
|---|---|---|---|
| Display and search blockchain data | Entity Information | • VASP: Holding address, account name, name of the country where the legal entity is located, current operating status, description of services, date of establishment, CEO name, brief description, contact information, e-mail address, country where the office is located, etc.<br>• DeFi/Wallet: address, account name, balance by token, last 24 hours trading volume, total sent/received, first/last active date, etc. | • Category names, account names, etc. labeled in the address can be obtained. |
| | Entity Transaction Information | • Transaction volume by VASP token, daily profit/loss amount, asset value, balance and transaction amount by address managed by VASP, transaction history, etc. | • Only VASPs are eligible. |
| | Entity Risk Information | • Countries of license registration, AML/KYC implementation status, etc. | • Only VASPs are eligible. |
| | Address risk level/risk score | • Risk level: 4 levels: Severe, High, Medium, and Low (severe: Risk score 80-100, High: risk score 50-79, etc.)<br>• Risk score: Risk value calculated on a scale of 100<br>*Information on risk determination: addresses used for fraud or crime in the past, addresses subject to sanctions, etc. | • Risk level classification and risk score values vary by analytics tools |
| | Description of high-risk transactions related to the address | • Reasons for determining that the transaction is high risk (threats, malware, mixing, darknet, phishing, ransomware, etc.)<br>• Graphical display of number of transactions, amount (USD, ETH, etc.), and number of transactions<br>• Transaction history (transaction date and time, transaction hash number, sender's address, recipient's address, amount, etc.)<br>• The above can be displayed by blockchain, time period, etc. | |
| | Listing of high-risk addresses | • Display addresses in order of risk score (link to view screen for each address) | |

# 3-3. Overview of Blockchain analytics tools

Table 3-3 Overview of Blockchain analytics tools (2/2)

| (data) item | Data and services provided | Specifics | Remarks |
|---|---|---|---|
| Display and search blockchain data | Transaction Graph | • Visualize the connection of transactions by drawing the transaction history by received/sent, category name/account name of sent/received address, token, and amount on one screen.<br>• Transactions associated with high-risk addresses are distinguished in red<br>• For a given address, automatically draw multiple transactions before and after in relation to each other<br>  | • Clicking on the appropriate icon (address) will display the sending/receiving transaction recipient, token name, amount, etc., centered on that address. |
| | Entity Related News | • Net news related to entities, etc. (excerpts of articles from various news sites) | |
| Trace Function | Automatic Transaction Tracing | • Automatically draws a series of multiple transactions executed for a specified address over a specified period of time<br>  | • When executed by specifying an address and period, the transaction status within the target period is continuously displayed. |
| Alert Detection | Automatic detection of designated address transactions | • Automatic detection and alert notification of transactions at specified addresses, including high-risk addresses | • By specifying the address in advance, the system automatically detects when a transaction occurs. |
| Sanctions List | View the list of sanctions for each country | • Display information (names of targets, details of sanctions, etc.) published in sanctions lists of U.S. OFAC, UK, EU, etc. | |
| Other | Record blockchain addresses | • A function that records a search address once and eliminates the need to enter the address the next time the search is performed. | |

# Chapter 4: Data Analysis Results

# Chapter 4: Data Analysis Results

- In this chapter, we present the results of actual analysis of the data pointed out in the previous chapters, obtained as much as possible by using analytical tools and researchers.
- This chapter is organized as follows
  - Section 4-1, Discuss the scope of the data analysis conducted and the limitations of the data analysis (in that there are many addresses and transactions that are difficult to analyze).
  - Section 4-2, Report the results of a quantitative comparison with other company's tools to examine the reliability of the data obtained from the researcher.
  - Section 4-3, Present the results of our data analysis focusing on the data availability and financial stability aspects of VASPs, lending platform, stablecoins, and DeFi, also taking into account the points raised in the FSB report.
  - Section 4-4, Present the distribution of VASPs, lending platform, unhosted wallets (including P2P), AML/CFT-related data availability, and high-risk transactions and the results of our analysis, taking into account the findings of the FATF report.

# 4-1. Scope and Limitations of Data Analysis

The scope of this research is limited to transaction data from addresses identified by the blockchain analytics company used in this study, including account names. As a result, the results of the data analysis are localized and limited to these data (the data of the entire decentralized financial system was not analyzed).

Table 4-1-1-1 Scope of survey for on-chain/off-chain data

| Item | Description | Supplement |
|---|---|---|
| **Scope of data research** | • Among the transaction data on the Ethereum blockchain in 2022, the blockchain analysis company have identified some addresses by category name (VASP, DeFi, etc.) or account name (VASP name, etc.), which were used as survey targets. The transaction data sent and received from these addresses were aggregated. | • The number of transactions identified by category or account name is 4-33% of the total and is not indicative of the total<br>• If the category names or other classifications identified by the blockchain analytics company are incorrect, the data will also be inaccurate. |

Figure 4-1-1 Scope of transaction data survey

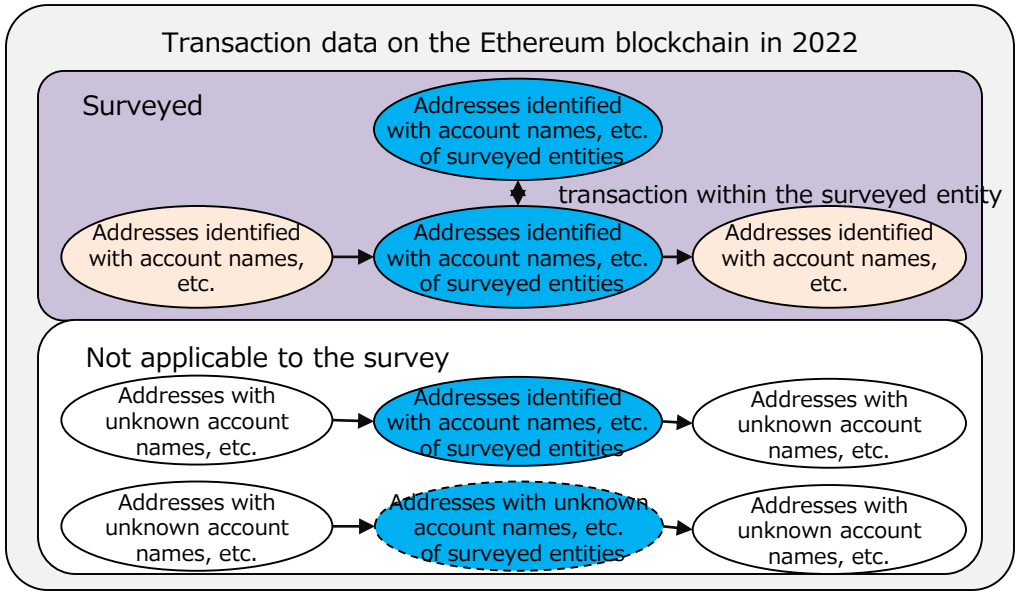



Table 4-1-1-2 Number of transactions for entities surveyed

| Surveyed Entity | Number of transactions | | | Ratio to the total number of Ethereum transactions* |
|---|---|---|---|---|
| | (1) Identified account name, etc. | (2) Unknown account name, etc. | (1) + (2)* | |
| VASP-A | 3,381,239 (13%) | 22,397,649 (87%) | 25,778,888 | 6.3% |
| VASP-B | 1,293,983 (4%) | 34,175,484 (96%) | 35,469,467 | 8.7% |
| Lending Platform | 144,457 (33%) | 297,820 (67%) | 442,277 | 0.1% |
| Unhosted Wallet | 5,772,973 (18%) | 26,097,100 (82%) | 31,870,073 | 7.8% |

*"(1)+(2)" is the number of transactions identified address holders, even if it is an unhosted wallet transaction.
*The number of transactions for the entire Ethereum in 2022: approx. 409 million.

# 4-2. Reliability Evaluation of Obtained Data

(1) Comparison of research results and other company's tools: A certain level of confidence in the number and value of VASP-related transactions

- There is a marked difference in the number of addresses held by the two companies, approximately 20~2,200 times. This may be due to the two companies different information collection resources and labeling methods.
- Since the difference between the two companies in terms of the number of transactions and transaction value is about 50-150%, which is not a large difference, a certain degree of reliability can be seen in the data.

→The above results suggest, for example, that (2) may contain surveyed entity-related addresses that are currently rarely used.

Table 4-2-1 Comparison of survey results and other company's tool

*Using token price rates as of April 2023.

| Item | Classification | | (1) Company A Research Results | (2) Company B Tool Information | (2) ÷ (1) | Remarks |
|---|---|---|---|---|---|---|
| VASP-A | Addresses | | 21,834 | 8,066,565 | 36945.0% | Significant difference (369x) |
| | Total Transfers | Incoming | 9,310,372 | 14,369,476 | 154.3% | |
| | | Outgoing | 14,269,851 | 12,135,550 | 85.0% | |
| | Total Volume (M$) | Incoming | 314,321 | 344,649 | 109.6% | |
| | | Outgoing | 311,188 | 340,245 | 109.3% | |
| VASP-B | Addresses | | 14,220 | 31,755,943 | 223318.9% | Significant difference (2,233x) |
| | Total Transfers | Incoming | 15,717,777 | 7,425,815 | 47.2% | |
| | | Outgoing | 18,752,632 | 13,616,799 | 72.6% | |
| | Total Volume (M$) | Incoming | 250,914 | 265,435 | 105.8% | |
| | | Outgoing | 252,892 | 255,632 | 101.1% | |
| Lending Platform | Addresses | | 15,730 | 306,442 | 1948.1% | Significant difference (19 x) |
| | Total Transfers | Incoming | 109,391 | 127,706 | 116.7% | |
| | | Outgoing | 205,940 | 202,160 | 98.2% | |
| | Total Volume (M$) | Incoming | 13,785 | 16,092 | 116.7% | |
| | | Outgoing | 11,725 | 16,288 | 138.9% | |

# 4-2. Reliability Evaluation of Obtained Data

(2) Comparison of research results with other company's tools: Reliability of data varies depending on trading partners.

- Since there is no significant difference in the number of transactions between the two VASPs and other VASPs, a certain degree of reliability can be seen in the data.
- The number of transactions/addresses between VASP and DeFi differs by a factor of about 3 between the two companies. This is thought to be due to differences in the way DeFi determines high-risk addresses between the blockchain analytics companies.

Table 4-2-2 Comparison of High-risk transactions survey results and other company's tool

| Item | Classification | Counterparty | Incoming / Outgoing | Total high-risk transfers (high-risk addresses)* | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | | (1) Company A Research Results | (2) Company B Tool Information | (2) ÷ (1) | |
| VASP-A | Addresses | - | - | 85 address | - | - | |
| | Total Transfers | In VASP-A | - | 2,184,570 (29 addresses) | 2,184,443 (17 addresses) | 99.9% (58.6%) | Difference (Number of addresses 2x) |
| | | VASP-B | VASP-A Incoming | 88,988 (18 addresses) | 88,983 (16 addresses) | 100.0 (88.9%) | |
| | | | VASP-A Outgoing | 59,102 (18 addresses) | 59,102 (18 addresses) | 100.0% (100.0%) | |
| | | Other VASPs | VASP-A Incoming | 173,577 (115 addresses) | 172,891 (99 addresses) | 99.6% (86.1%) | |
| | | | VASP-A Outgoing | 133,483 (398 addresses) | 116,634 (136 addresses) | 87.4% (34.2%) | Difference (Number of addresses 3x) |
| | | DeFi | VASP-A Incoming | 30,158 (262 addresses) | 9,954 (132 addresses) | 33.0% (38.8%) | Difference (Trx. 3x, Addr. 3x) |
| | | | VASP-A Outgoing | 3,465 (37 addresses) | 3,383 (21 addresses) | 96.4% (82.3%) | |
| | | Unhosted Wallet | VASP-A Incoming | 11,565 (55 addresses) | 10,561 (32 addresses) | 91.3% (58.2%) | Difference (Number of addresses 2x) |
| | | | VASP-A Outgoing | 25,622 (131 addresses) | 19,561 (58 addresses) | 76.3% (44.3%) | Difference (Number of addresses 2x) |

*The number of addresses is the total of both sending and receiving addresses; (2) is the number of high-risk transactions and addresses in (1) that are high-risk using the tools of blockchain analytics company B.

# 4-2. Reliability Evaluation of Obtained Data

(3) Comparison of research results with other company's tools: Reliability of data varies depending on trading partners.

- There is a marked difference in the number of high-risk transactions/addresses for unhosted wallets between the two analytics companies. This suggests that there are significant differences in the identification rate of unhosted wallets and the method used to determine high-risk addresses among the analytics companies.

Table 4-2-3 Comparison of High-risk transactions survey results and other company's tool

| Item | Classification | Counterparty | Incoming / Outgoing | Total high-risk transfers (high-risk addresses)* | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | | (1) Company A Research Results | (2) Company B Tool Information | (2) ÷ (1) | |
| VASP-B | Addresses | - | - | 8 addresses | - | - | |
| | Total Transfers | In VASP-B | - | 694,838 (8 addresses) | 694,838 (8 addresses) | 100.0% (100.0%) | |
| | | VASP-A | (Same as the number of transactions in VASP-A / VASP-B) | | | | |
| | | Other VASPs | VASP-B Incoming | 45,792 (56 addresses) | 45,744 (55 addresses) | 100.0% (98.2%) | |
| | | | VASP-B Outgoing | 51,716 (211 addresses) | 47,144 (57 addresseses) | 91.2% (27.0%) | Difference (Number of addresses 4x) |
| | | DeFi | VASP-B Incoming | 4,039 (102 addresses) | 2,464 (60 addresses) | 61.0% (58.8%) | Difference (Trx. 2x, Addr. 2x) |
| | | | VASP-B Outgoing | 361 (14 addresses) | 356 (10 addresses) | 98.6% (71.4%) | |
| | | unhosted wallet | VASP-B Incoming | 3,467 (31 addresses) | 3,264 (21 addresses) | 94.1% (67.7%) | Difference (Number of addresses 1.5x) |
| | | | VASP-B Outgoing | 22,259 (105 addresses) | 20,157 (39 addresses) | 90.6% (37.1%) | Difference (Number of addresses 3x) |
| Unhosted Wallet | Addresses | - | - | 291 addresses | - | - | |
| | Total Transfers | P2P transactions | - | 425,882 (291 addresses) | 15,349 (55 addresses) | 3.6% (18.9%) | Significant difference (Trx. 28x, Addr. 5x) |

*The number of addresses is the total of both sending and receiving addresses; (2) is the number of high-risk transactions and addresses in (1) that are high-risk using the tools of blockchain analytics company B.

# 4-2. Reliability Evaluation of Obtained Data

(4) Key Findings

Table 4-2-4 Key Findings

| Key Findings | | Contents | Supplement |
|---|---|---|---|
| Limitations of Blockchain Analytics Tools | Only in a small percentage of cases can the counterparty be identified. | • Of all the transactions conducted with related addresses of the surveyed (VASPs, etc.), only a small portion of the transactions were able to identify the counterparties (i.e., categories of sending/receiving addresses, account names, etc.).<br>• Reasons may include difficulty in obtaining sufficient information to identify categories and accounts (e.g., addresses with only one transaction in the past), insufficient capacity of analytics tool companies (not enough off-chain data available to identify addresses, such as IP addresses, web traffic, and sanctions-related information), etc. | • It is possible that more counterparties were identified by other company's analytics tools. However, there is a possibility that the identification is based on insufficient data, and it is difficult to judge the superiority of the analytics company based solely on the identification rate. |
| | Data exist that show marked differences among analytics tool companies. | • While there are data categories where the differences between the two companies, such as the number and value of transactions between VASPs, are slight and can be given a certain degree of credibility, the results show marked differences between the analytics tool companies, such as the number of addresses held by VASPs and DeFi/unhosted wallet-related transactions.<br>• The reason for the relatively high confidence in VASP-related transactions may be that VASPs, where transactions above a certain size are concentrated, may be easier to identify than unhosted wallet-related transactions (including P2P), where transactions are held by individuals and are considered sporadic.<br>• Other differences in labeling methods (heuristic-based: based on empirical rules, etc. or proprietary algorithms, etc.) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

- With regard to the points raised in the FSB report, the results of an investigation into the possibility of data acquisition using various tools and expert research confirmed that some of the data made available in the report were difficult to obtain using the methods of this research, and that it was possible to obtain some of the data that was said to be unavailable (including data with limited obtaining).
- Note that the results of this survey are only localized based on the analytical tools used in this study and the results of expert research.

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (1/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Wealth Effects | Available Metrics | Market capitalization of crypto-assets | △<br>Major crypto assets can be obtained | △<br>Major crypto assets can be obtained | ×<br>Difficult to obtain data | △<br>Major crypto assets can be obtained | Targets are crypto assets whose market capitalization is disclosed by crypto asset-related databases, etc. |
| | | | Trading volumes | △<br>Can be obtained from the crypto asset issuer's transaction data on a per transaction basis. (aggregation is difficult). | ×<br>Difficult to obtain data | △<br>Can be obtained from the crypto asset issuer's transaction data on a per transaction basis. (aggregation is difficult). | ○<br>Can be obtained from the crypto asset issuer's transaction data | Targets are addresses identified by blockchain analytics companies as unbacked crypto-assets |
| | | | Realized volatility and gamma | ×<br>Difficult to obtain data | ▲<br>Price fluctuation data can be obtained and may be calculated from said data. | ×<br>Difficult to obtain data | -<br>(Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (2/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Wealth Effects | Available Metrics | Geographical adoption | × Difficult to obtain data | × Difficult to obtain data | ▲ Data on the countries of registration of the main VASP licenses and available crypto assets can be obtained | - (Not included in this survey) | Some blockchain analytics companies that were not used in this research have published reports on regional penetration |
| | | Data Gaps | Share of households invested in crypto assets | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Share of assets relative to household wealth | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Demographic skew among household's holdings | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Owners of unbacked crypto assets | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Certain types of users are identified, such as major exchanges, prominent investors and sanctioned users. |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (3/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Confidence Effects | Available Metrics | Share of retail ownership of crypto assets | ▲<br>It is difficult to calculate the share because it is limited to a part of the address account names, etc. that are specified. | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>It is difficult to calculate the share because it is limited to a part of the address account names, etc. that are specified. | Targets are addresses identified as account names, etc. by blockchain analytics companies |
| | | | Number of clients in infrastructures that provide access to crypto assets (e.g. trading platforms, wallet providers) | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | -<br>(Not included in this survey) | Platformers and wallet providers may have it as internal data. |
| | | Data Gaps | Volume of crypto asset fraud | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>Some fraud cases have been identified, but it is difficult to calculate the total amount | ▲<br>Some fraud cases have been identified, but it is difficult to calculate the total amount | Targets are addresses identified as fraudulent transactions by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (4/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Financial Sector Exposure | Available Metrics | Share of institutional ownership of crypto assets | ▲ Institutional holdings are limited to identified addresses, making it difficult to calculate overall share | × Difficult to obtain data | ▲ Institutional holdings are limited to identified addresses, making it difficult to calculate overall share | ▲ Institutional holdings are limited to identified addresses, making it difficult to calculate overall share | |
| | | | Share of assets invested in crypto assets | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Number of large financial service providers offering crypto asset services | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | It is considered possible to ascertain a certain level of information through information on registered operators in each country. |
| | | | Volume of crypto asset derivatives market | × Difficult to obtain data | △ Main crypto assets can be obtained. | × Difficult to obtain data | △ Main crypto assets can be obtained. | |
| | | | Open interest of crypto asset derivative contracts | × Difficult to obtain data | △ Main crypto assets can be obtained. | × Difficult to obtain data | △ Main crypto assets can be obtained. | |
| | | | Correlations of crypto assets with other asset classes | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in the survey) | |
| | | | Share of transaction volume by transaction size | ▲ Limited to some addresses such as identified by account name, etc., and difficult to ascertain the share of transactions. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc., and difficult to ascertain the share of transactions. | ▲ Limited to some addresses such as identified by account name, etc., and difficult to ascertain the share of transactions. | Targets are addresses identified as financial institutions by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (5/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Financial Sector Exposure | Data Gaps | AUM and share of holdings of funds that offer exposure to crypto assets (by asset type e.g. spot, derivative, eco system and investor type) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Bank sector exposure (absolute vs hedged; change in open interest) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Reporting by financial institutions on crypto assets held and serviced | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (6/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Use in Payments and Settlements | Available Metrics | Prices and delta (over one week, 1m, 3m, 6m, 1y) | × Difficult to obtain data | △ Main token prices and trends can be obtained. | × Difficult to obtain data | △ Major Token Prices and Transition Available | |
| | | | Trading volumes (absolute vs. average) | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as payment services by blockchain analytics companies |
| | | | Number of large payment service providers supporting crypto assets | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | Certain public information about registered operators exists. |
| | | | Market share of major crypto-asset exchanges | × Difficult to obtain data | ○ Possibility to calculate market share from trading volume by crypto asset pair for major VASPs | × Difficult to obtain data | ○ Possibility to calculate market share from trading volume by crypto asset pair for major VASPs | Crypto asset related databases to obtain the last 24 hours trading volume, etc. |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(1) Data availability for unbacked crypto-assets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-1 Data availability for unbacked crypto-assets (7/7)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Unbacked crypto-assets | Use in Payments and Settlements | Data Gaps | Number and value of transactions | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as payment services by blockchain analytics companies |
| | | | Jurisdiction of the payers and payees | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. and jurisdiction (e.g., VASP) | ▲ Limited to some addresses such as identified by account name, etc. and jurisdiction (e.g., VASP) | Targets are addresses identified with account name and jurisdiction, etc. by blockchain analytics companies |
| | | | Type of transactions (e.g. remittances, ecommerce, trading) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Types of crypto assets employed | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Acceptance as legal tender | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(2) Data availability for stablecoins

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-2 Data availability for stablecoins (1/6)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Stablecoins | Wealth Effects | Available Metrics | Market capitalization of stablecoins | ○<br>(Assumption of equivalence to pegged legal tender) | △<br>Major stablecoins can be ontained | ×<br>Difficult to obtain data | ○<br>(Assumption of equivalence to pegged legal tender) | Targets are stablecoins whose market capitalization is disclosed by crypto asset-related databases, etc. |
| | | | Trading volumes | △<br>Can be obtained from stablecoin issuer transaction data on a per transaction basis (difficult to aggregate) | ×<br>Difficult to obtain data | △<br>Can be obtained from stablecoin issuer transaction data on a per transaction basis (difficult to aggregate) | ○<br>Can be obtained from stablecoin issuer transaction data | Targets are addresses identified as stablecoins by blockchain analytics companies |
| | | | Realized volatility | ×<br>Difficult to obtain data | ▲<br>Price fluctuation data can be obtained and may be calculated | ×<br>Difficult to obtain data | -<br>(Not included in this survey) | |
| | | Data Gaps | Owners of stablecoins | ▲<br>Limited to a portion of the address account name identified. | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>Limited to some addresses such as identified by account name, etc. | Targets are to addresses identified as account names, etc. by blockchain analytics companies |
| | | Data to be added | Business relationship between VASP and issuers of stablecoins | △<br>Limited to VASPs identified on the BC Explorer and obtained on a per transaction basis (difficult to aggregate) | ×<br>Difficult to obtain data | △<br>Limited to VASPs identified by the analytics tool and can be obtained on a per transaction basis (difficult to aggregate) | △<br>A certain number can be obtained only for the VASPs identified by the analytics tool | Targets are addresses identified as VASP by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(2) Data availability for stablecoins

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-2 Data availability for stablecoins (2/6)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Stablecoins | Confidence Effects | Available Metrics | Share of retail ownership of stablecoins | ▲<br>Limited to some addresses such as identified by account name, etc. | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>Limited to some addresses such as identified by account name, etc. | Targets are addresses identified by blockchain analytics companies as account names, etc. |
| | | | Number of clients in infrastructures that provide access to stablecoins (e.g. trading platforms, wallet providers) | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | -<br>(Not included in this survey) | Platformers and wallet providers may have it as internal data. |
| | | Data Gaps | Volume of crypto asset fraud | △<br>Can be obtained from transaction data of addresses with past fraudulent transactions on a per transaction basis (difficult to aggregate) | ×<br>Difficult to obtain data | △<br>Can be obtained from transaction data of addresses with past fraudulent transactions on a per transaction basis (difficult to aggregate) | ○<br>Can be obtained from transaction data of addresses with past fraudulent transactions | Targets are addresses identified as fraudulent transactions by blockchain analytics companies |
| | | Data to be added | Addresses to be frozen / total amount subject to be frozen | △<br>Can be obtained from stablecoin issuer transaction data on a per transaction basis (difficult to aggregate) | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ○<br>Can be obtained from stablecoin issuer transaction data | Aggregate addresses and volume of transactions with "Blocked" transaction results for stablecoin issuers |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(2) Data availability for stablecoins

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-2 Data availability for stablecoins (3/6)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Stablecoins | Financial Sector Exposure | Available Metrics | Share of institutional ownership of stablecoins | ▲ Institutional holdings are limited to identified addresses, making it difficult to calculate overall share | × Difficult to obtain data | ▲ Institutional holdings are limited to identified addresses, making it difficult to calculate overall share | ▲ Institutional holdings are limited to identified addresses, making it difficult to calculate overall share | |
| | | | Share of assets invested in stablecoins | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in the survey) | |
| | | | Number of large financial service providers offering stablecoin services | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | It is considered possible to ascertain a certain level of information through information on registered operators in each country. |
| | | | Size of stablecoin market relative to US prime money market funds | × Difficult to obtain data | △ Stablecoin market size is obtainable Market size of US MMFs is difficult to obtain | × Difficult to obtain data | ○ The size of the market for stablecoin and US MMFs can be obtained. | |
| | | Data Gaps | Amounts and share of holdings of ETFs that offer exposure to stablecoins (by investor type) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Profit and loss exposures | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(2) Data availability for stablecoins

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-2 Data availability for stablecoins (4/6)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Stablecoins | Financial Sector Exposure | Data Gaps | Reserve assets invested in regulated Markets / Liquidity of reserve assets / granular and robust data on composition of stablecoins reserve assets | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Reporting by financial institutions on crypto assets held and serviced | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | Data to be added | Actual crypto asset transactions by institutional investors and financial institutions (e.g., types of crypto assets/ stablecoins preferred by large users) | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as institutional investors or financial institutions by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(2) Data availability for stablecoins

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-2 Data availability for stablecoins (5/6)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Stablecoins | Use in Payments and Settlements | Available Metrics | Prices | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | ○ Token price to be used for payment can be obtained from payment service websites, etc. | Investigate the possibility of obtaining a token price when used in payments. |
| | | | Number of transactions | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as payment services by blockchain analytics companies |
| | | | Number of large payment service providers supporting stablecoins | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(2) Data availability for stablecoins

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-2 Data availability for stablecoins (6/6)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| Stablecoins | Use in Payments and Settlements | Data Gaps | Number and value of transactions | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as payment services by blockchain analytics companies |
| | | | Jurisdiction of the payers and payees | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. and jurisdiction (e.g., VASP) | Limited to some addresses such as identified by account name, etc. and jurisdiction (e.g., VASP) | Targets are addresses identified with account name and jurisdiction, etc. by blockchain analytics companies |
| | | | Type of transactions (e.g. remittances, e commerce, trading) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Usage in crypto asset trading platforms, by stablecoin | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Breakdown of uses of stablecoins | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (1/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Wealth Effects | Available Metrics | Total value locked in, gross, adjusted and net; realized volatility | × Difficult to obtain data | △ Main DeFi can be obtained. | × Difficult to obtain data | △ Main DeFi can be obtained. | Targets are DeFi for which crypto asset-related databases and other data are publicly available |
| | | | Transaction volume of DeFi's Exchange (DEX) | ▲ Transactions for each address identified as DEX can be obtained for each transaction, but it is difficult to aggregate the number of transactions. | × Difficult to obtain data | ▲ Transactions for each address identified as DEX can be obtained for each transaction, but it is difficult to aggregate the number of transactions. | △ A certain number of transaction data for addresses identified as DEX can be obtained. | Targets are addresses identified as DEX by blockchain analytics companies |
| | | | Wallet growth | × Difficult to obtain data | × Difficult to obtain data | ▲ Transactions for some addresses identified as unhosted wallets can be obtained on a per transaction basis (historical transaction data can be obtained). | ▲ Historical trend data can be obtained for transactions at some addresses identified as unhosted wallets | Investigate the feasibility of obtaining data on the number of transactions and amount of money in unhosted wallets using DeFi. |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (2/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Rxperts | |
| DeFi | Wealth Effects | Available Metrics | Market capitalization and transaction volume of governance tokens | △<br>Market capitalization of major tokens can be obtained<br>Number of transactions can be obtained per transaction (difficult to aggregate) | △<br>Market capitalization of major tokens can be obtained<br>Number of transactions is difficult to obtain | △<br>Market capitalization of major tokens is difficult to obtain<br>Number of transactions can be obtained per transaction (difficult to aggregate) | ○<br>Market capitalization and number of transactions for major tokens can be obtained. | Major governance tokens for which crypto-asset related databases, etc., publish market capitalization |
| | | | Transaction volume in DeFi Lending / Lending rate in DeFi Lending | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>Some DeFi can be obtained. | May be obtained from the website of the relevant DeFi lending service |
| | | | Utilization rate of liquidity pool of DeFi Lending and Exchange | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | -<br>(Not included in this survey) | |
| | | | DeFi yield and return | ×<br>Difficult to obtain data | △<br>DeFi yields can be obtained, but return is difficult to obtain | ×<br>Difficult to obtain data | -<br>(Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (3/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Wealth Effects | Data Gaps | Share of retail vs institutional participation | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as account names, etc. by blockchain analytics companies |
| | | | Number of dApps on a blockchain | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | ▲ Major DApps have been identified and it may be possible to aggregate a certain number of DApps, but research costs are high | Data can be obtained by some BC Explorers (DappRadar, etc.) |
| | | | Liquidity pools, DeFi stablecoins, derivatives (entities within the DeFi space, including types of financial institutions (specialized or traditional financial institutions) to understand linkages of DeFi with the rest of the financial system) | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as financial institutions by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (4/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Wealth Effects | Data Gaps | Metrics to measure leverage | ▲<br>Some DeFi can be obtained. | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>Some DeFi can be obtained. | Investigate the feasibility of obtaining data on overall DeFi liabilities/assets, etc. |
| | | | Information on the governance tokens holders could be obtained from to see to what extent the governance is decentralized (e.g. if the ownership of governance tokens is concentrated, that entity could be considered the actual developer) | ▲<br>Limited such as identified by account name, etc. of the holder address.<br>Dispersion of token holdings by address can be obtained. | ×<br>Difficult to obtain data | ×<br>Difficult to obtain data | ▲<br>Limited such as identified by account name, etc. of the holder address.<br>Dispersion of token holdings by address can be obtained. | Targets are addresses identified as account names, etc. by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (5/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Wealth Effects | Data to be added | TVL (TVL-based market share of major DeFi protocols) | × Difficult to obtain data | △ Main DeFi can be obtained. | × Difficult to obtain data | △ Main DeFi can be obtained. | DeFi for which crypto asset-related databases and other data are publicly available. |
| | | | Market Capitalization of Stablecoins | △ Major stablecoins can be obtained | △ Major stablecoins can be obtained | × Difficult to obtain data | △ Major stablecoins can be obtained | Targets are stablecoins whose market capitalization is disclosed by crypto asset-related databases, etc. |
| | | | Degree of linkage between major DeFi (DEX-Lending, etc.) | △ Transaction data between major DeFi's can be obtained on a per transaction basis (difficult to aggregate) | × Difficult to obtain data | △ Transaction data between major DeFi's can be obtained on a per transaction basis (difficult to aggregate) | ○ Transaction data between major DeFi's can be obtained. | |
| | | | Total tokens locked in cross-chain bridge | △ The major bridges can be obtained | × Difficult to obtain data | × Difficult to obtain data | △ The major bridges can be obtained | Targets are addresses identified as bridges by blockchain analytics companies |
| | | | Cross Chain Bridge's business relationship with VASP | △ Transaction data between main DeFi and bridge can be obtained on a per transaction basis (difficult to aggregate) | × Difficult to obtain data | × Difficult to obtain data | △ A certain number of transaction data for addresses identified as bridges and VASPs can be obtained. | Targets are addresses identified as VASP by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (6/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Wealth Effects | Data to be added | Oracle's market share in TVL and other measures | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Collateral ratios, leverage ratios, and actual rehypothecation according to collateral type for lending protocols | ▲ Some DeFi can be obtained. | × Difficult to obtain data | × Difficult to obtain data | ▲ Some DeFi can be obtained. | |
| | | | Major remittance address from Treasury Protocol | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as Treasury Protocol by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (7/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Confidence Effects | Available Metrics | Number of clients in infrastructures that provide access to DeFi (e.g. trading platforms, wallet providers) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | Information from stablecoin operators is considered necessary. |
| | | Data Gaps | Volume of crypto asset fraud | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as fraudulent transactions by blockchain analytics companies |
| | | | Share of transactions in unbacked crypto assets vs. stablecoins | △ Transaction data for major crypto assets and stablecoins can be obtained on a per transaction basis. (difficult to aggregate) | × Difficult to obtain data | △ Transaction data for major crypto assets and stablecoins can be obtained on a per transaction basis. (difficult to aggregate) | △ A certain number of major crypto assets and stablecoin transaction data can be obtained. | Targets are addresses identified as unbacked crypto-assets or stablecoins by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (8/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Confidence Effects | Data to be added | Governance Token Concentration | △ Transaction data for each of the major governance tokens can be obtained (difficult to aggregate) | × Difficult to obtain data | × Difficult to obtain data | △ Transaction data for major governance tokens can be obtained. | Targets are Addresses identified as governor's tokens by blockchain analytics companies |
| | | | DeFi Protocol Concentration | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | △ Number and value of transactions by main DeFi can be obtained. | Targets are addresses identified as DeFi protocols by blockchain analytics companies |
| | | | Total amount and number of DeFi-related hacking losses | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | △ Total damage and number of major hacking incidents can be obtained. | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (9/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Financial Sector Exposure | Available Metrics | Share of institutional ownership of crypto assets | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as institutional by blockchain analytics companies |
| | | | Share of assets invested in crypto assets | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | Difficulty in acquiring a ratio of crypto assets held by financial institutions |
| | | | Number of large financial service providers offering crypto asset services | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Volume of crypto asset derivatives market | × Difficult to obtain data | △ Main DeFi can be obtained. | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Open interest of derivative contracts | × Difficult to obtain data | △ Main DeFi can be obtained. | × Difficult to obtain data | - (Not included in this survey) | |
| | | | Correlations of crypto assets with other asset classes | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | Difficult to obtain data on crypto assets in financial institutions' assets |
| | | | Share of transaction volume by transaction size | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as financial institutions by blockchain analytics companies |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (10/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Financial Sector Exposure | Data Gaps | Amounts and share of holdings of ETFs that offer exposure to crypto assets by investor type | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |
| | | Data to be added | Amount invested in traditional financial assets utilizing tokens locked to smart contracts as collateral | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-1. Availability of Data as Indicated by the FSB Report

(3) Data availability for DeFi

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-3-1-3 Data availability for DeFi (11/11)

| Classification | Transmission Channels | Data Classification | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|---|
| | | | | BC Explorer | Crypto Asset Related Database | Blockchain Analytics Tools | Research by Experts | |
| DeFi | Use in Payments and Settlements | Available Metrics | Price of key players (DOT, UNI, LINK) | × Difficult to obtain data | △ Main token prices can be obtained. | × Difficult to obtain data | △ Main token prices can be obtained. | Investigate the possibility of obtaining the main token prices used in payments |
| | | | Delta over one week, one month, three months, six months, one year and 7 day average volume | × Difficult to obtain data | △ Main token price increase/decrease can be obtained. | × Difficult to obtain data | △ Main token price increase/decrease can be obtained. | |
| | | Data Gaps | Number and value of transactions | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as payment services by blockchain analytics companies |
| | | | Jurisdiction of the payers and payees | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. and jurisdiction (e.g., VASP) | Targets are addresses identified as account names, etc. by blockchain analytics companies |
| | | | Type of transactions (e.g. remittances, ecommerce, trading) | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | - (Not included in this survey) | Data on transaction type is difficult to obtain |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-2. Research Survey Items

- In this chapter, specific survey items such as the number of address holders and the number and value of transactions were set for each category of VASPs and lending platform for the following four survey items, which were researched by experts from a blockchain analysis company.
- The research results were organized into tables and graphs after organizing the data, and the trends and characteristics seen in the results were discussed.

Table 4-3-2 Research survey items

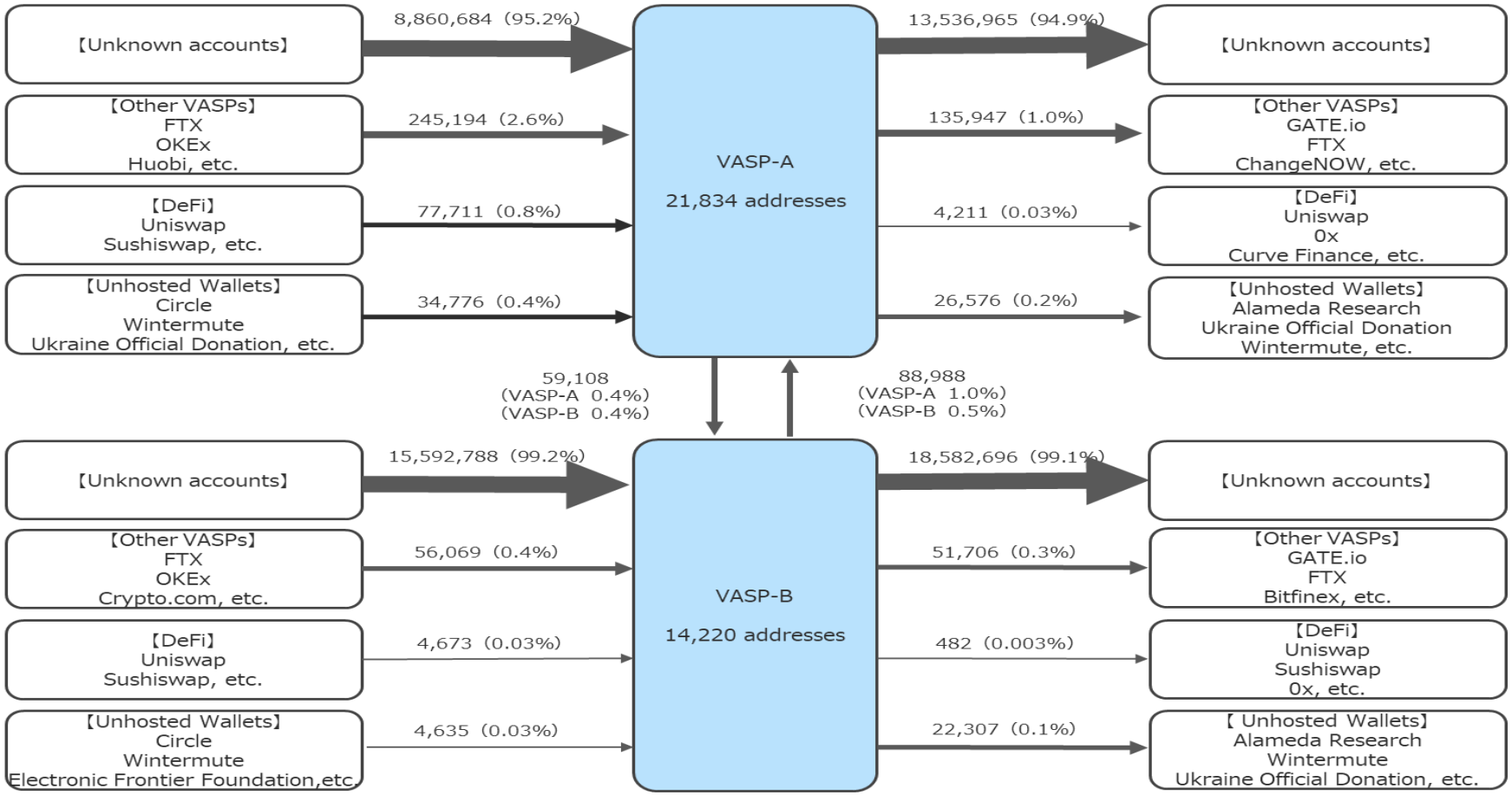
| Survey items | Survey Contents | supplement |
|---|---|---|
| Trends in the number of transactions of major VASPs | • The number and value of transactions for the two major VASPs were surveyed in three categories: incoming, within their own company, and outgoing.<br>• Three categories were investigated: (1) by category, (2) by DeFi, and (3) by token breakdown among the categories. | • Account category names and account names used classifications defined by the blockchain analytics company.<br>• DeFi service types were defined by us based on public information on the Web.<br>• The transaction amount used the token price and other rates as of April 2023. |
| Trends in the number of transactions by major lending platform | • The number of transactions and the amount of transactions were surveyed for one major lending platform in three categories: incoming, within their own company, and outgoing.<br>• Three categories were investigated: (1) by category, (2) by DeFi, and (3) by token breakdown among the categories. | |
| Stablecoin related data | • The actual remittance status and frozen transaction data were surveyed for three major stablecoins (USDC, USDC, and DAI). | |
| DeFi related data | • For the major DeFi projects (Uniswap, Maker, and Aave), we surveyed the size of the DeFi, the number of governor's token holders, collateral ratios, and rehypothecation (collateral diversion).<br>• As part of a survey of the overall DeFi situation, we investigated the status of cross-chain bridge usage, hacking damage, cooperation with financial institutions, and the degree of concentration on specific oracle services. | |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-3. Major VASPs

(1) Main VASPs: Summary of the number of transactions by VASP-A/VASP-B

- Among the transactions that could be identified, many were between VASPs, suggesting a close linkage of exchanges, etc. In addition, transactions between VASPs and DeFi, and between VASPs and stablecoin issuers/investment companies, etc., were also identified (included in unhosted wallets by definition), suggesting the possibility of a close business relationship among them.
- It should be noted that the results of this analysis do not necessarily represent the overall trend related to VASPs, as the number of transactions with addresses where the account name or other information is unknown accounted for more than 95% of the total number of transactions.

Figure 4-3-3-1 Summary of major VASP transactions



# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-3. Major VASPs (VASP-A)

(2) Major VASPs: VASP-A by Category

Figure 4-3-3-2 VASP-A number of transactions / amount by category

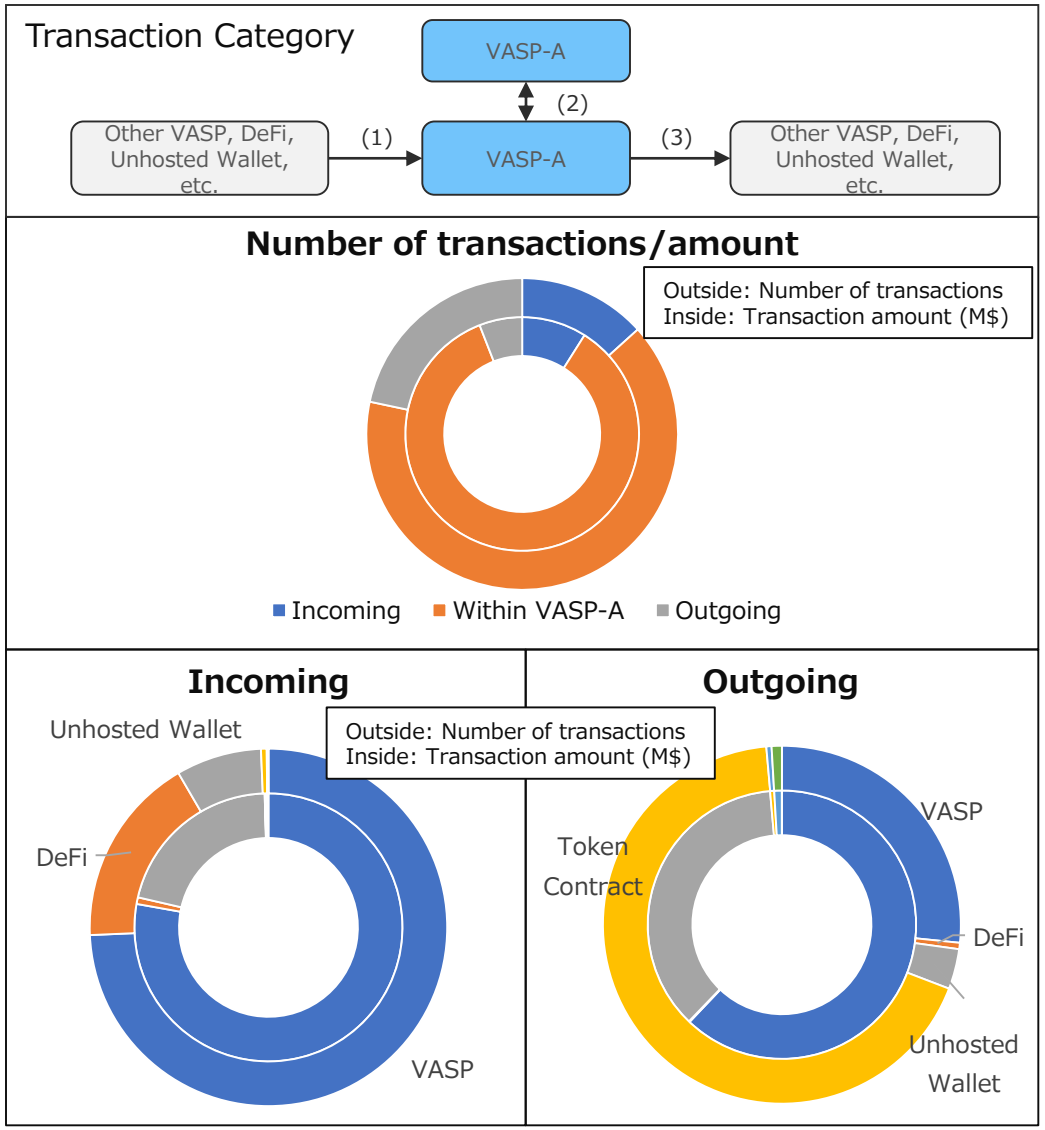



Table 4-3-3-2 VASP-A transactions / amount data by category

| Transaction Category | Account Category | Number of transactions | | Amount of transaction | |
|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Amount Ratio |
| (1) Incoming | VASP | 334,182 | 74.3% | 51,239 | 77.8% |
| | DeFi | 77,711 | 17.3% | 528 | 0.8% |
| | Unhosted Wallet | 34,776 | 7.7% | 13,791 | 20.9% |
| | Token Contract | 2,320 | 0.5% | 27 | 0.0% |
| | Bridge | 566 | 0.1% | 148 | 0.2% |
| | Other | 133 | 0.0% | 123 | 0.2% |
| | Total | 449,688 | 100.0% | 65,856 | 100.0% |
| (2) Within VASP-A | VASP | 2,198,665 | 100.0% | 625,406 | 100.0% |
| | Total | 2,198,665 | 100.0% | 625,406 | 100.0% |
| (3) Outgoing | VASP | 195,055 | 26.6% | 27,079 | 62.1% |
| | DeFi | 4,211 | 0.6% | 46 | 0.1% |
| | Unhosted Wallet | 26,576 | 3.6% | 15,873 | 36.4% |
| | Token Contract | 496,837 | 67.8% | 217 | 0.5% |
| | Bridge | 3,451 | 0.5% | 398 | 0.9% |
| | Other | 6,756 | 0.9% | 0 | 0.0% |
| | Total | 732,886 | 100.0% | 43,613 | 100.0% |

[Discussion]

- "(2) Within VASP-A" is the largest number of transactions within transaction categories.
  → Are most of them due to internal fund transfers of wallets.
- "(1) Incoming" is for other VASPs, and "(3) Outgoing" are for token contracts and VASPs, which account for the majority of the number of transactions.
  A certain number of DeFi and unhosted wallet transactions are also recognized.
  → Token contracts are transfers of tokens compliant with ERC-20 standards (e.g., 62% of all transfers are USDT transfers, but the transaction amounts are small and may be partially double-counted with actual transfers (counted in a different category such as VASP)),
  DeFi is intended for DEX use, while unhosted wallets may be intended for subsequent DeFi use, etc.?

# 4-3. Results of Financial Stability-Related Data Analysis
# 4-3-3. Major VASPs (VASP-A)

## (3) Major VASPs: VASP-A DeFi breakdown among Category

Figure 4-3-3-3 VASP-A number of transactions / amount by DeFi

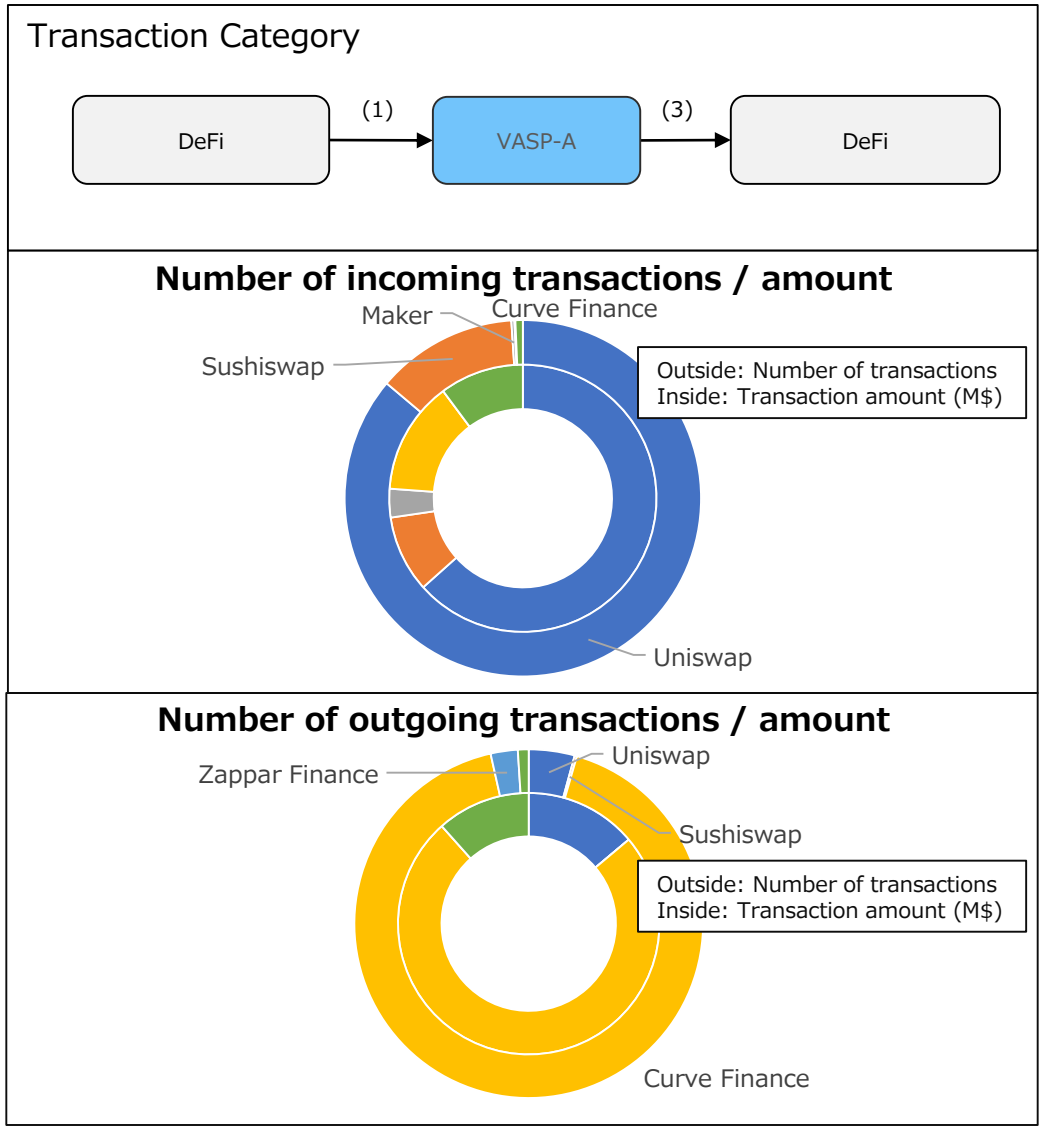



Table 4-3-3-3 VASP-A transactions / amount data by DeFi

| DeFi | Service | (1) Incoming | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ |
| Uniswap | Ddecentralized Exchange | 66,954 | 86.2% | 335 | 179 | 4.3% | 6 |
| Sushiswap | Decentralized Exchange | 9,955 | 12.8% | 49 | 9 | 0.2% | 0 |
| Maker | Stablecoins Issuance | 215 | 0.3% | 18 | 0 | 0.0% | 0 |
| Curve Finance | Decentralized Exchange | 65 | 0.1% | 72 | 3,875 | 92.0% | 34 |
| Zappar Finance | DeFi Dashboard | 1 | 0.0% | 0 | 106 | 2.5% | 0 |
| Other | - | 521 | 0.7% | 54 | 42 | 1.0% | 5 |
| Total amount | | 77,711 | 100.0% | 528 | 4,211 | 100.0% | 46 |

[Discussion]

- DeFi has large number of transactions and amount on decentralized exchanges (over 95% of total).
  → Decentralized exchanges are thought to have more crypto asset exchanges and staking remittances.
- Among decentralized exchanges, Uniswap has the highest number of transactions for “(1) Incoming” and Curve Finance for “(3) Outgoing”.
  → The reasons are not necessarily clear, but Uniswap exchanges many types of tokens (about 800 types), Curve Finance is used for exchanging stablecoins, etc.?

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-3. Major VASPs (VASP-A)

(4) Major VASPs: VASP-A by Token

Figure 4-3-3-4 VASP-A number of transactions / amount by token

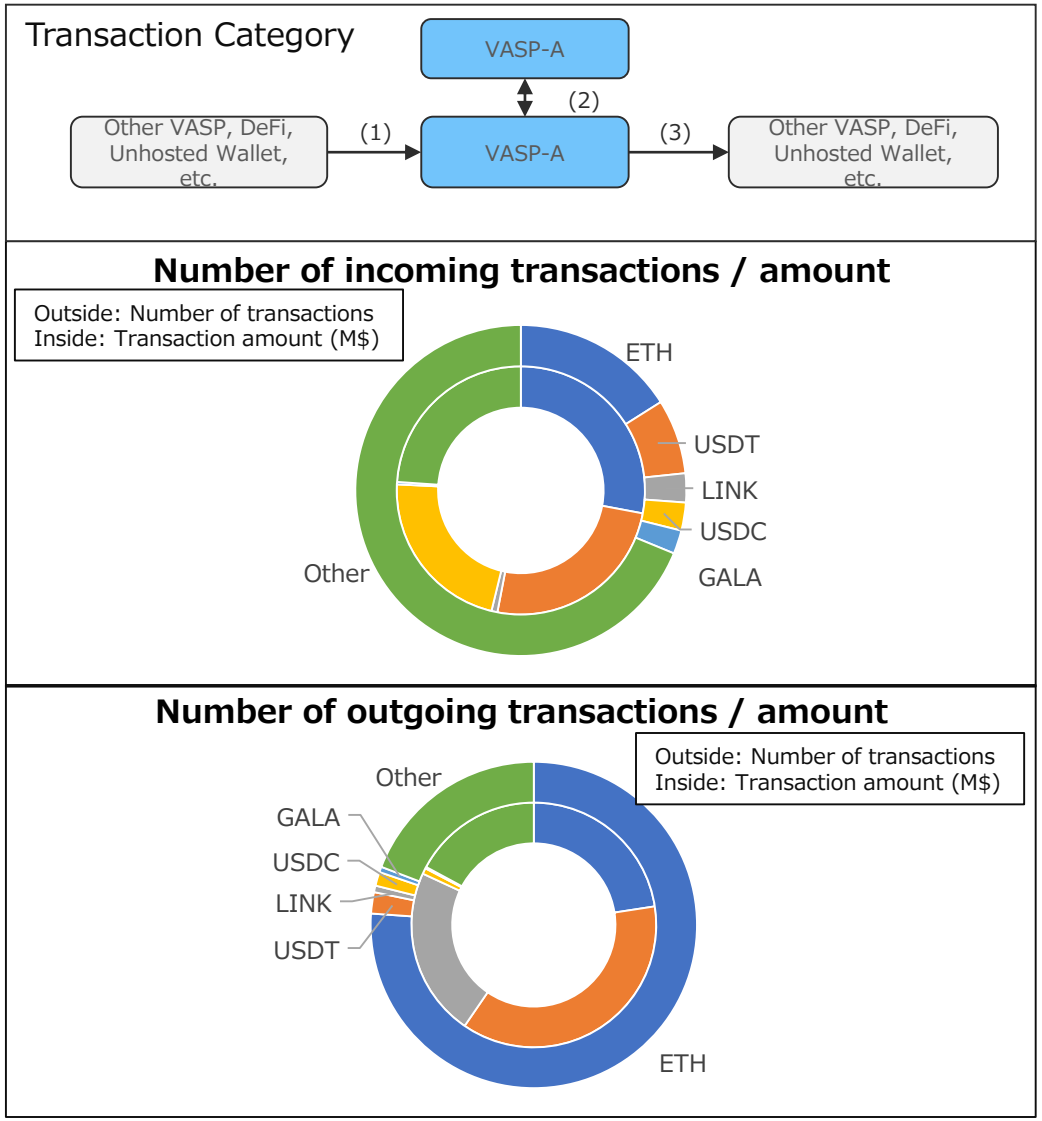



Table 4-3-3-4 VASP-A transactions / amount data by token

| Token | Classification | (1) Incoming | | | (2) Within VASP-A | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ |
| ETH | Native Token | 72,095 | 16.0% | 18,416 | 1,581,015 | 71.9% | 196,040 | 557,875 | 76.1% | 9,845 |
| USDT | Stablecoins | 32,849 | 7.3% | 16,509 | 84,191 | 3.8% | 164,185 | 15,463 | 2.1% | 16,135 |
| LINK | For External Oracles | 12,744 | 2.8% | 513 | 15,317 | 0.7% | 84,536 | 4,769 | 0.7% | 9,736 |
| USDC | Stablecoins | 12,319 | 2.7% | 14,470 | 18,349 | 0.8% | 4,396 | 10,120 | 1.4% | 336 |
| GALA | For use in Games | 10,337 | 2.3% | 208 | 11,500 | 0.5% | 2,300 | 3,924 | 0.5% | 89 |
| Other | - | 309,344 | 68.8% | 15,740 | 488,293 | 22.2% | 173,949 | 140,735 | 19.2% | 7,473 |
| Total | | 449,688 | 100.0% | 65,856 | 2,198,665 | 100.0% | 625,406 | 732,886 | 100.0% | 43,613 |

*1) "Other" in incoming refers to the number of transactions for approximately 1,100 types of tokens.

[Discussion]

- ETH, USDT, and USDC have the large number and amount of transactions.
  → This may be due to the fact that these tokens are often used as major tokens and exchanged for other tokens, etc.
- ETH has the largest number and amount of transactions in “(1) Incoming” and ”(2) Within VASP-A”. In “(3) Outgoing”, ETH has the highest number of transactions, USDT has the largest transaction amount. USDT has a higher amount per transaction than the others.
  → ETH and USDT are considered to be used more for fund transfers with other VASPs.
- LINK (external oracle service Chainlink use token) has a large number of transactions.
  → This is considered to be due to the large number of DeFi that use Chainlink, an external oracle service.
- GALA (Gala Games’ game usage token) has a next large number o transactions.
  → Possibly due to the use of this game (Gala Games: total supply of 39 billion tokens and 230,000 addresses of token holders as of May 2011).

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-3. Major VASPs (VASP-B)

### (5) Major VASPs: VASP-B by Category

Figure 4-3-3-5 VASP-B number of transactions / amount by category

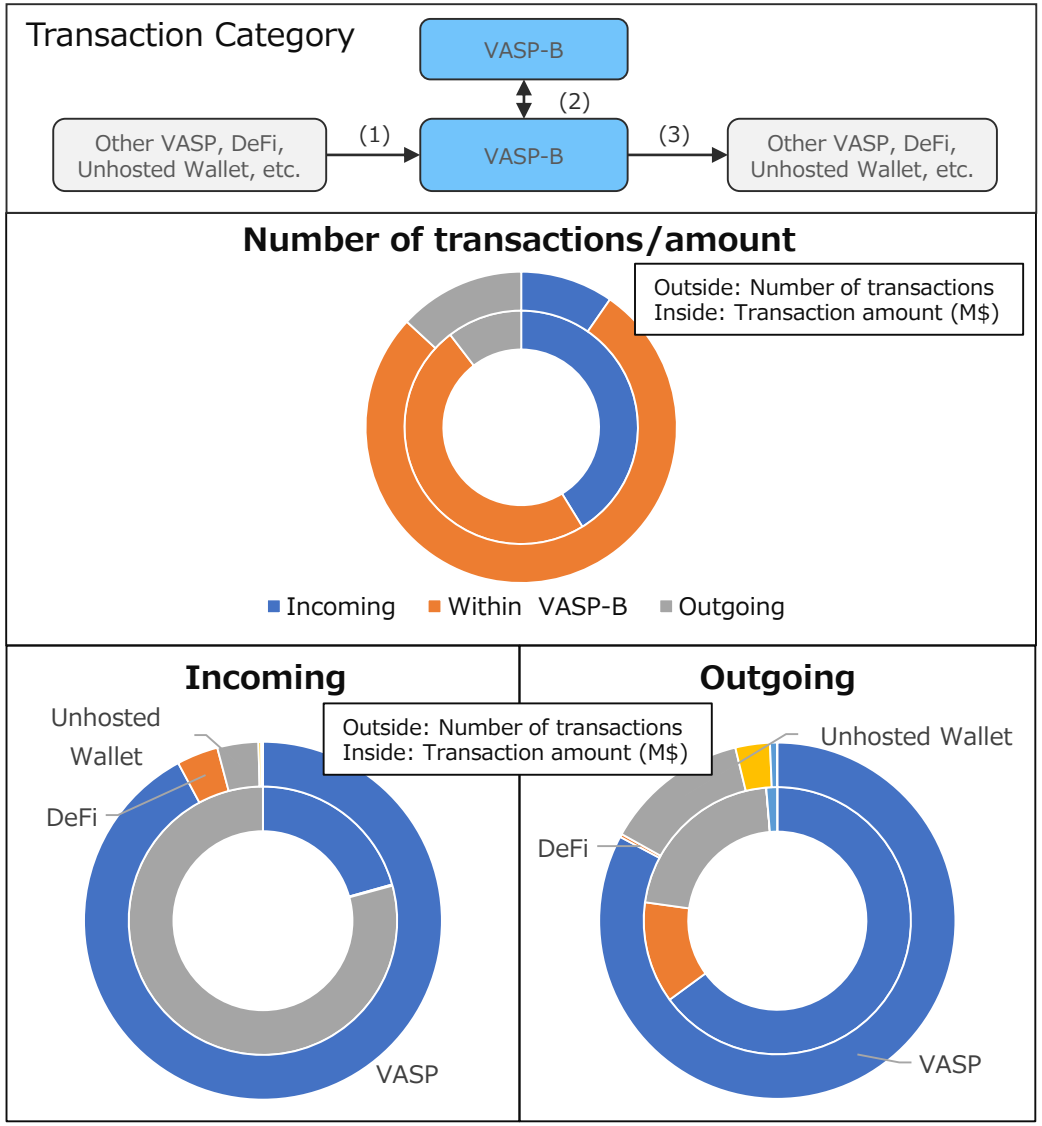



Table 4-3-3-5 VASP-B transactions / amount data by category

| Transaction Category | Account Category | Number of transactions | | Amount of transaction | |
|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Amount Ratio |
| (1) Incoming | VASP | 115,177 | 92.1% | 17,190 | 20.6% |
| | DeFi | 4,673 | 3.7% | 123 | 0.1% |
| | Unhosted Wallet | 4,635 | 3.7% | 65,944 | 79.2% |
| | Token Contract | 306 | 0.2% | 0 | 0.0% |
| | Bridge | 192 | 0.2% | 1 | 0.0% |
| | Other | 6 | 0.0% | 0 | 0.0% |
| | Total | 124,989 | 100.0% | 83,259 | 100.0% |
| (2) Within VASP-B | VASP | 999,058 | 100.0% | 97,707 | 100.0% |
| | Total | 999,058 | 100.0% | 97,707 | 100.0% |
| (3) Outgoing | VASP | 140,704 | 82.8% | 13,655 | 64.9% |
| | DeFi | 482 | 0.3% | 2,583 | 12.3% |
| | Unhosted Wallet | 22,307 | 13.1% | 4,514 | 21.5% |
| | Token Contract | 5,320 | 3.1% | 1 | 0.0% |
| | Bridge | 1,072 | 0.6% | 279 | 1.3% |
| | Other | 51 | 0.0% | 0 | 0.0% |
| | Total | 169,936 | 100.0% | 21,032 | 100.0% |

[Discussion]
- "(2) Within VASP-B" is the largest number of transactions within transaction categories.
  → Most of them are due to internal fund transfers of wallets within VASP.
- Other than within-VASP-B transactions, the majority of transactions with other VASPs accounted for both "(1) Incoming" and "(3) Outgoing" transactions.
  → Most of the funds are considered to be transferred to other major VASPs.
- The next large number of transactions are DeFi and Unhosted Wallets for "(1) Incoming" and Unhosted Wallets for "(3) Outgoing".
  → DeFi is the token exchange for decentralized exchanges, while Unhosted Wallets are considered for DeFi use, etc.?
- Unhosted Wallets is the largest amount of transactions within "(1) Incoming".
  → Could this mean that funds from the VASP wallet were used for DeFi services, etc. through a Unhosted Wallet?

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-3. Major VASPs (VASP-B)

(6) Major VASPs: VASP-B DeFi breakdown among Category

Figure 4-3-3-6 VASP-B number of transactions / amount by DeFi

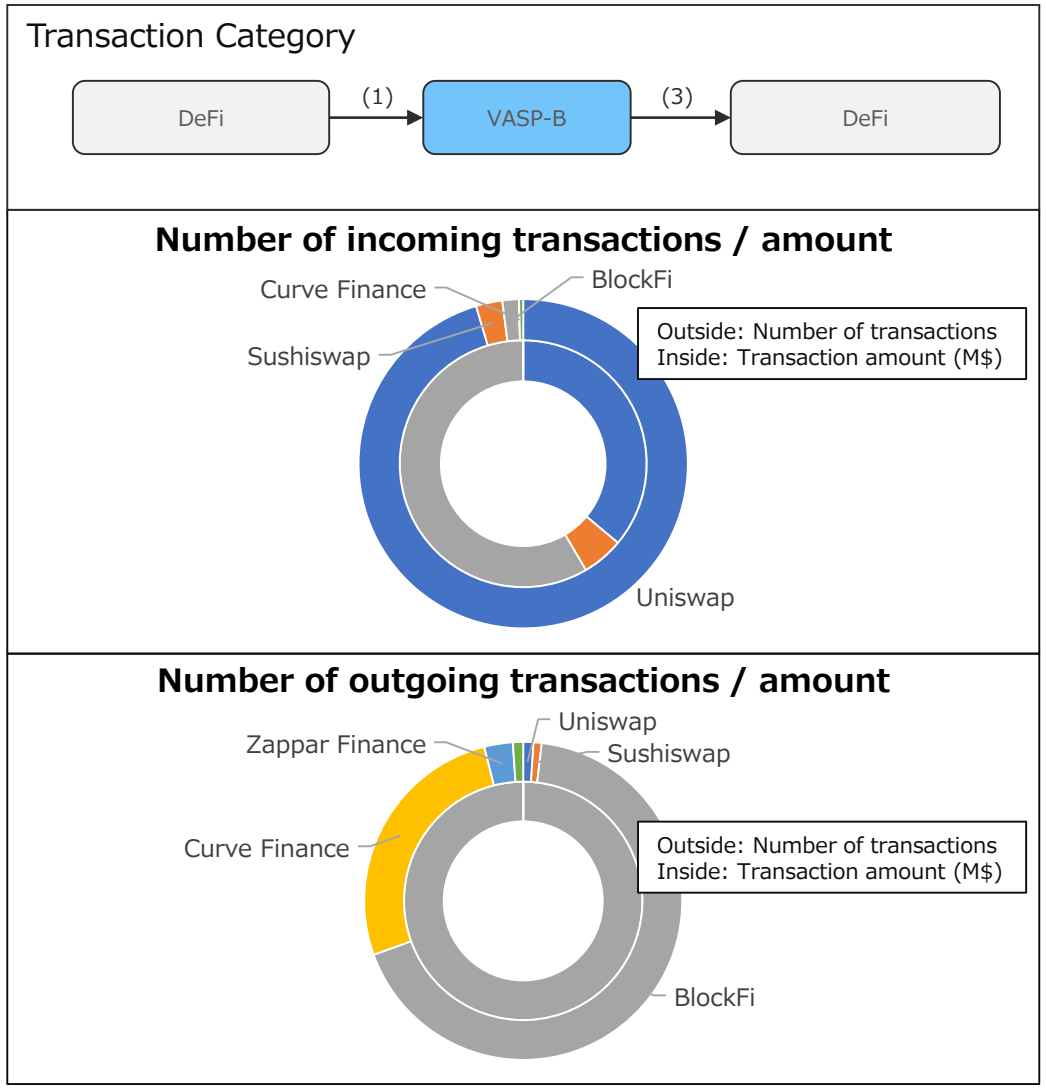



Table 4-3-3-6 VASP-B transactions / amount data by DeFi

| DeFi | Service | (1) Incoming | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ |
| Uniswap | Decentralized Exchange | 4,457 | 95.4% | 19 | 5 | 1.0% | 0 |
| Sushiswap | Decentralized Exchange | 121 | 2.6% | 3 | 4 | 0.8% | 0 |
| BlockFi | Lending Platform | 76 | 1.6% | 30 | 326 | 67.6% | 2,583 |
| Curve Finance | Decentralized Exchange | 0 | 0.0% | 0 | 128 | 26.6% | 0 |
| Zappar Finance | DeFi Dashboard | 0 | 0.0% | 0 | 14 | 2.9% | 0 |
| Other | - | 19 | 0.4% | 0 | 5 | 1.0% | 0 |
| total amount | | 4,673 | 100.0% | 52 | 482 | 100.0% | 2,583 |

[Discussion]

- The large number of transactions are decentralized exchanges for "(1) Incoming" and lending platform for "(3) Outgoing".
  → Decentralized exchanges are considered to be due to the exchange of crypto assets and remittance of staking, while lending platform is considered to be due to the use of crypto asset lending services.
- Among decentralized exchanges, Uniswap for “(1) Incoming” and Curve Finance for “(3) Outgoing” have large number of transactions.
  → Uniswap is used for exchanging many types of tokens (about 800 types), and Curve Finance is used for exchanging stablecoins?

# 4-3. Results of Financial Stability-Related Data Analysis
# 4-3-3. Major VASPs (VASP-B)

## (7) Major VASPs: VASP-B by Token

Figure 4-3-3-7 VASP-B number of transactions / amount by token

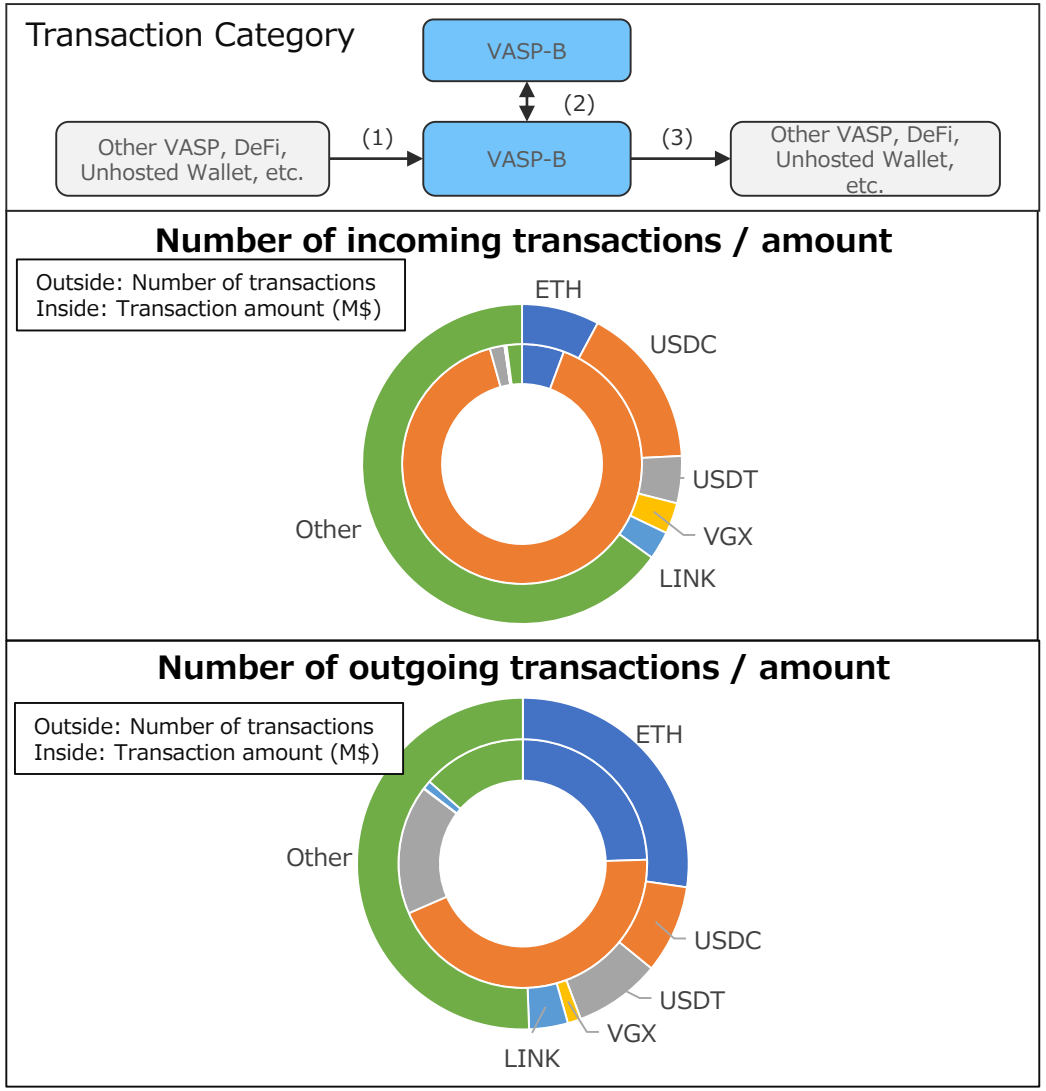



Table 4-3-3-7 VASP-B transactions / amount data by Token

| Token | Classification | (1) Incoming | | | (2) Within VASP-B | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ |
| ETH | Native token | 9,804 | 7.8 | 4,723 | 848,157 | 84.9% | 9,345 | 46,376 | 27.3% | 5,155 |
| USDC | Stablecoins | 20,433 | 16.3% | 74,866 | 45,016 | 4.5% | 82,798 | 14,612 | 8.6% | 9,249 |
| USDT | Stablecoins | 5,957 | 4.8% | 1,636 | 16,371 | 1.6% | 3,031 | 14,333 | 8.4% | 3,541 |
| VGX | VASP-issued tokens | 3,922 | 3.1% | 47 | 3,411 | 0.3% | 54 | 2,201 | 1.3% | 14 |
| LINK | For External Oracles | 3,563 | 2.9% | 203 | 5,038 | 0.5% | 391 | 6,424 | 3.8% | 233 |
| Other | - | 81,310 | 65.1% | 1,713 | 81,065 | 8.1% | 2,100 | 85,990 | 50.6% | 2,845 |
| Total | | 124,989 | 100.0% | 83,188 | 999,058 | 100.0% | 97,719 | 169,936 | 100.0 | 21,038 |

*1) "Other" in incoming refers to the number of transactions for approximately 600 types of tokens.

[Discussion]

- ETH, USDT, and USDC have a large number of transactions in all transaction categories.
  → This may be due to the fact that these tokens are often used as major tokens and exchanged for other tokens.
- VGX (tokens issued by VASP Voyager) has a large number of transactions.
  → Probably due to fund transfers between major VASPs.
  (As of May 2011: total supply of 290 million tokens, 6,500 addresses of token holders)
- LINK (external oracle service Chainlink use token) has a next large number of transactions.
  → This is considered to be due to the large number of DeFi that use Chainlink, an external oracle service.

# 4-3. Results of Financial Stability-Related Data Analysis
# 4-3-4. Major Lender

## (1) Major Lending Platform: By Category

Figure 4-3-4-1 Lending Platform number of transactions / amount by category

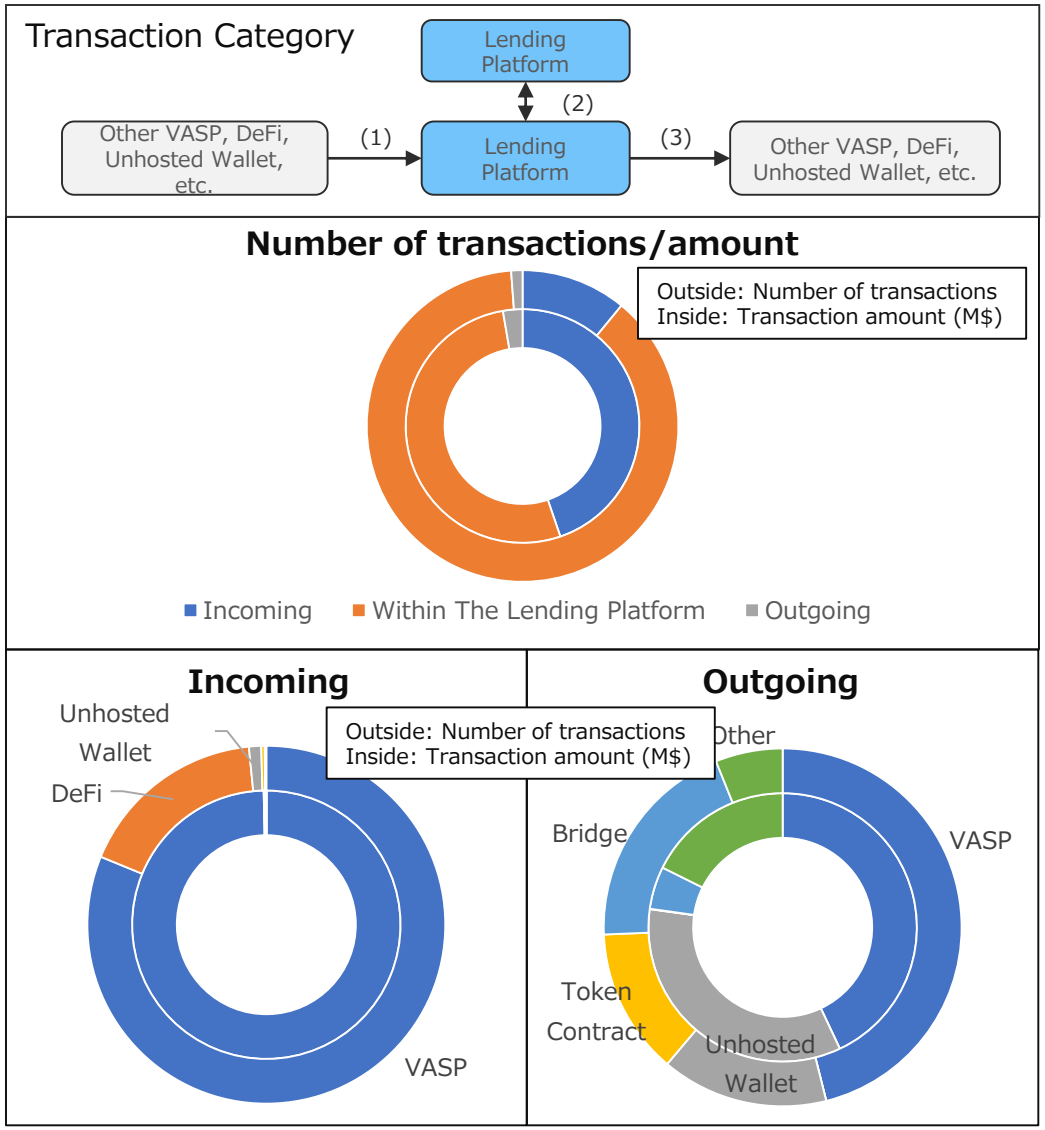



Table 4-3-4-1 Lending Platform transactions / amount data by category

| Transaction Category | Account Category | Number of transactions | | Amount of transaction | |
|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | Amount M$ | Amount Ratio |
| (1) Incoming | VASP | 12,841 | 81.2% | 6,807 | 99.7% |
| | DeFi | 2,727 | 17.2% | 6 | 0.1% |
| | Unhosted Wallet | 174 | 1.1% | 15 | 0.2% |
| | Token Contract | 50 | 0.3% | 0 | 0.0% |
| | Bridge | 12 | 0.1% | 0 | 0.0% |
| | Other | 10 | 0.1% | 0 | 0.0% |
| | Total | 15,814 | 100.0% | 6,828 | 100.0% |
| (2) Within the Lending Platform | Lending Platform | 126,946 | 100.0% | 8,015 | 100.0% |
| | Total | 126,946 | 100.0% | 8,015 | 100.0% |
| (3) Outgoing | VASP | 782 | 46.1% | 177 | 43.0% |
| | DeFi | 0 | 0.0% | 0 | 0.0% |
| | Unhosted Wallet | 256 | 15.1% | 141 | 34.2% |
| | Token Contract | 224 | 13.2% | 0 | 0.0% |
| | Bridge | 332 | 19.6% | 21 | 5.1% |
| | Other | 103 | 6.1% | 73 | 17.6% |
| | Total | 1,697 | 100.0% | 412 | 100.0% |

[Discussion]

- “(2) Within The Lending Platform” is the largest number of transactions within transaction categories.
  → Likely due to internal fund transfers of wallets within their own services.
- Among the transaction categories, the number of transactions in “(1) Incoming” is larger than that in “(3) Outgoing”.
  → The number of transactions in “(1) Incoming” is considered to be higher due to the use of crypto asset lending platform, while the number of transactions in “(3) Outgoing” is considered to be lower due to the withdrawal of funds.
- By category, the number of transactions with other VASPs is large for both “(1) Incoming” and “(3) Outgoing”. The next large number of transactions were DeFi for “(1) Incoming” and Unhosted Wallets such as custodians, etc. for “(3) Outgoing”.
  → Although the background is not necessarily clear, it is possible that the use of staking services for crypto assets, for example, is a possible purpose of utilization.

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-4. Major Lending Platform

(2) Major Lending Platform: DeFi Breakdown among Category

Figure 4-3-4-2 Lending Platform number of transactions / amount by DeFi

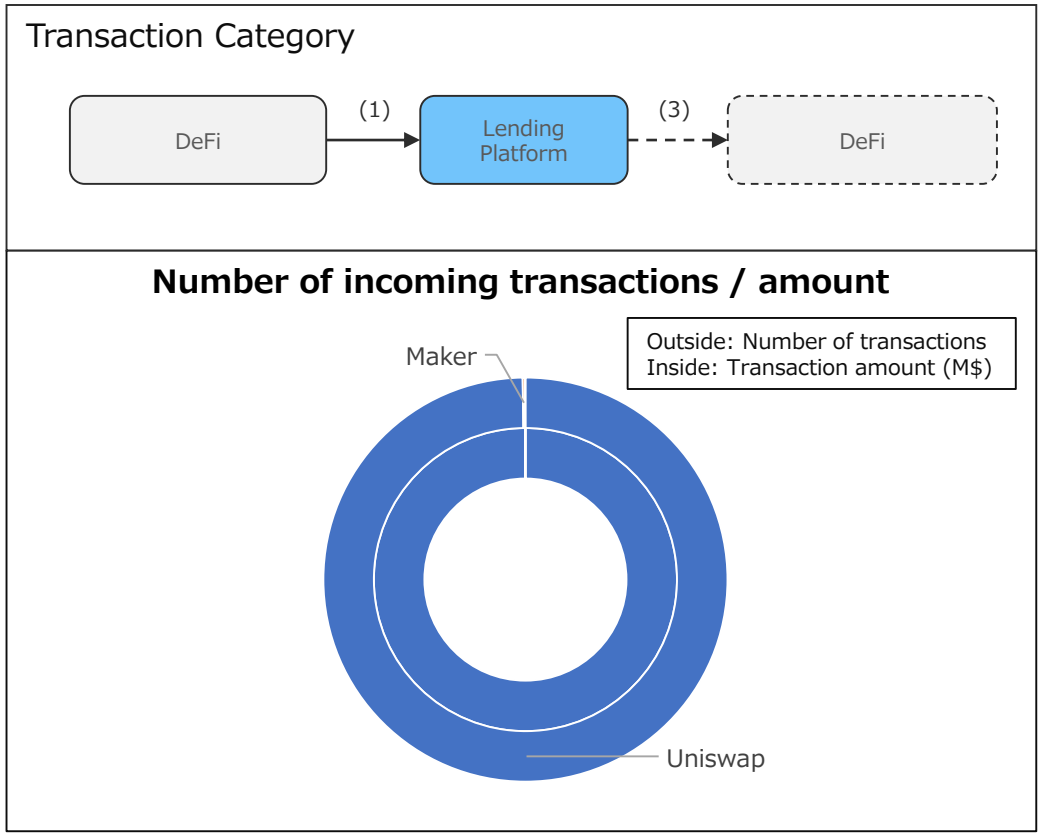



Table 4-3-4-2 Lending Platform transactions / amount data by DeFi

| DeFi | Service | (1) Incoming | | |
|---|---|---|---|---|
| | | transactions | Transaction ratio | amount M$ |
| Uniswap | Decentralized Exchange | 2,721 | 99.8% | 6 |
| Maker | Stablecoins Issuance | 5 | 0.2% | 0 |
| Compound | Lending | 1 | 0.0% | 0 |
| total amount | | 2,727 | 100.0% | 6 |

*"(3) Outgoing" is not applicable transaction.

[Discussion]

- "(1) Incoming" are mostly traded on decentralized exchanges.
  → This is considered to be due to multi token transfers (approx. 300 types).
- "(1) Incoming" and "(3) Outgoing" are different.
  → This is considered to be due to the large number of transactions on decentralized exchanges.

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-4. Major Lending Platform

(3) Major Lending Platform: By Token

Figure 4-3-4-3 Lending Platform number of transactions / amount by DeFi

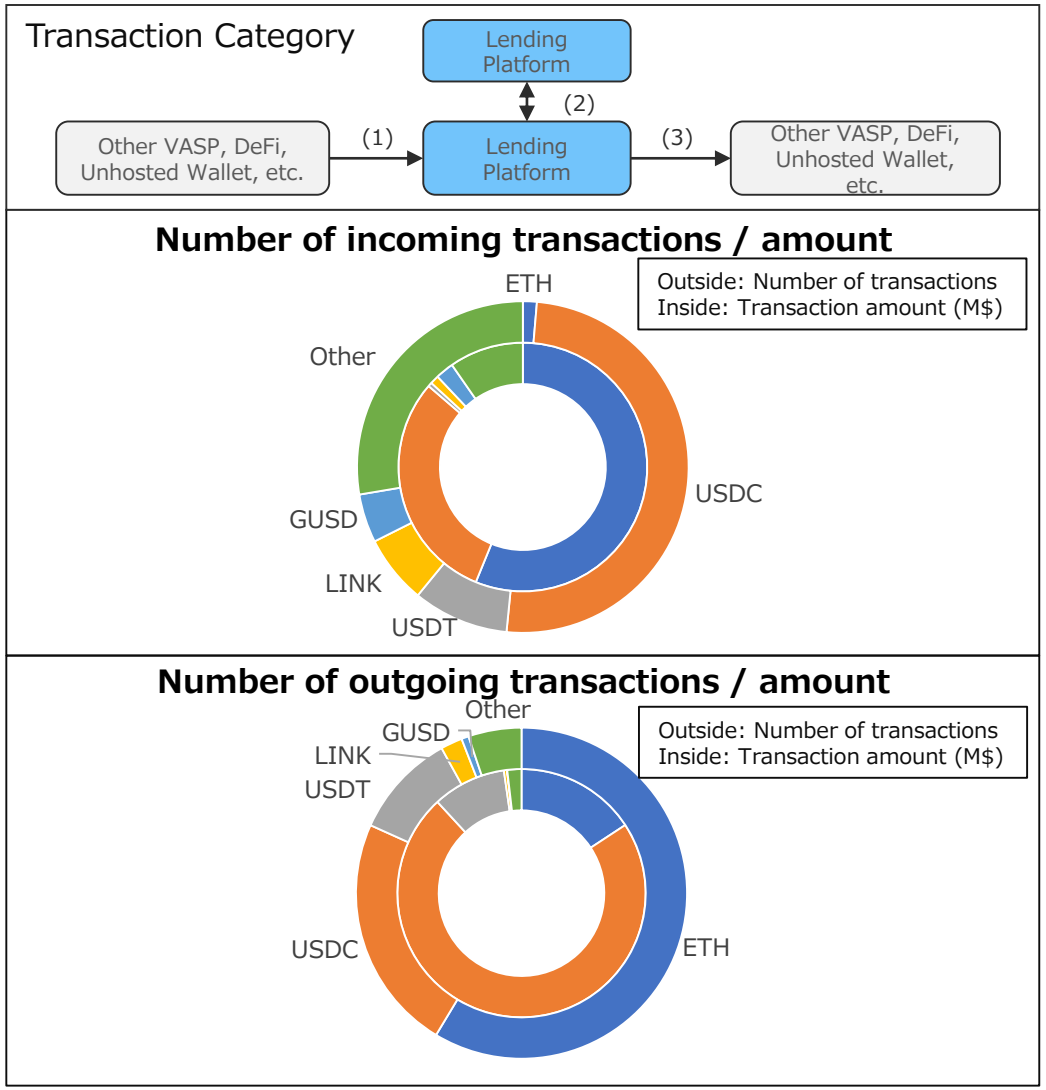



Table 4-3-4-3 Lending Platform transactions / amount data by Token

| Token | Classification | (1) Incoming | | | (2) Within The Lending Platform | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | transactions | Transaction ratio | amount M$ | transactions | Transaction ratio | amount M$ | transactions | Transaction ratio | amount M$ |
| ETH | Native token | 215 | 1.4% | 3,836 | 77,958 | 61.4% | 2,346 | 995 | 58.6% | 65 |
| USDC | Stablecoins | 7,941 | 50.2% | 2,057 | 29,412 | 23.2% | 3,784 | 392 | 23.1% | 298 |
| USDT | Stablecoins | 1,478 | 9.3% | 36 | 4,932 | 3.9% | 994 | 174 | 10.3% | 39 |
| LINK | For External Oracles | 1,057 | 6.7% | 78 | 2,614 | 2.1% | 117 | 36 | 2.1% | 2 |
| GUSD | Stablecoins | 750 | 4.7% | 162 | 5,474 | 4.3% | 476 | 12 | 0.7% | 0 |
| Other | - | 4,373 | 27.7% | 659 | 6,556 | 5.2% | 298 | 88 | 5.2% | 8 |
| Total | | 15,814 | 100.0% | 6,828 | 126,946 | 100.0% | 8,015 | 1,697 | 100.0% | 412 |

*1) "Other" in incoming is the number of transactions for about 300 types of tokens.

[Discussion]

- ETH, USDT, and USDC have a large number of transactions in all transaction categories.
  → This may be due to the fact that these tokens are often used as major tokens and exchanged for other tokens.
- LINK (external oracle service Chainlink use token) has a large number of transactions.
  → This is considered to be due to the large number of DeFi that use Chainlink, an external oracle service.
- GUSD (token issued by VASP Gemini) has a next large number of transactions.
  → This is considered to be due to fund transfers within VASPs.
  (GUSD: total supply 540 million tokens, token holders 10,000,000 addresses as of May 23)

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-5. Stablecoins Related

- While there were some trends among the three types of stave coins surveyed, in general, the overwhelming majority of stave coin use was confirmed to be on DeFi.
- No actual cases of address freezing could be confirmed for DAI, an algorithmic stave coin (possibility that the freezing function does not exist).
- Unhosted wallets were observed to have more destination addresses but fewer transactions in number and amount than DeFi and VASP. This may be due to the fact that DeFi and VASP transactions are concentrated in specific remittance destinations (e.g., DEX major VASPs).

Table 4-3-5 Stablecoins Data Survey Results

| Category | Surveyed Items | Surveyed Data | On-chain data survey results | | | Remarks |
|---|---|---|---|---|---|---|
| | | | USDC Stablecoins | USDT Stablecoins | DAI Stablecoins | |
| Stablecoins Related | Actual status of stablecoin remittance (main use cases, remittance scale, etc.) | Remittance Addresses | 2,057 Addresses<br>【Breakdown】<br>Unhosted Wallet 1,020,<br>Token Contract 698,<br>VASP 128, etc. | 1, 657 Addresses<br>【Breakdown】<br>Unhosted Wallet 689,<br>Token Contract 630,<br>VASP 151, etc. | 899 Addresses<br>【Breakdown】<br>Unhosted Wallet 321,<br>Token Contract 311,<br>VASP 105, etc. | |
| | | Number of transactions and amount of transactions at the above addresses | 7,966,000 TRX/<br>1,402.1 billion USD<br>【Breakdown】<br>DeFi<br>4.059 million TRX/<br>751.4 billion USD,<br>VASP<br>1.95 million TRX/<br>1.1 billion USD,<br>Unhosted Wallet<br>615,000 TRX/<br>138.1 billion USD, etc. | 8,093,000 TRX/<br>236.2 billion USD<br>【Breakdown】<br>VASP<br>5.109 million TRX/<br>2.6 billion USD,<br>DeFi<br>1.865 million TRX/<br>93.4 billion USD,<br>Unhosted Wallet<br>188,000 TRX/<br>21.5 billion USD, etc. | 1,272,000TRX /<br>509.5 billion USD<br>【Breakdown】<br>DeFi<br>648,000 TRX/<br>428.2 billion USD,<br>VASP<br>193,000 TRX/<br>0.08 billion USD,<br>Unhosted Wallet<br>87,000 TRX/<br>19.3 billion USD, etc. | |
| | Data related to stave coins frozen by the issuing entity (addresses subject to freezing, total amount frozen, etc.) | Addresses subject to freeze | 159 addresses | 858 addresses | - | As of April 2023 |
| | | Total frozen amount/average amount per address | 7,859,000 USD/<br>21 addresses<br>Average 374,000 USD | 440 million USD/<br>777 addresses<br>Average 567,000 USD | - | As of April 2023 |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-6. DeFi Related

(1) DeFi related

Table 4-3-6-1 Results of DeFi data survey (1/2)

| Category | Surveyed Items | Surveyed Data | On-chain data survey results | | | Remarks |
|---|---|---|---|---|---|---|
| | | | Uniswap Decentralized Exchange | Maker Stablecoin Issuance | Aave Lending Protocol | |
| DeFi Related | Overall size of DeFi (TVL, number of users, market capitalization of stabled coins, etc.) | TVL per DeFi | 4.09 billion USD (UNI) | 7.23 billion USD (DAI) | USD 5.18 billion (AAVE) | As of May 2023 |
| | | Number of token/stablecoin holders | (Listed in the Governance Token column) | 507,000 addresses (DAI) | (Listed in the Governance Token column) | As of May 2023 |
| | | Market capitalization of tokens/stablecoins | 2.94 billion USD (UNI) | 4.98 billion USD (DAI) | 940 million USD (AAVE) | As of May 2023 |
| | DeFi vulnerabilities (e.g., governance tokens and DeFi protocol concentration) | Number of Governance token holder addresses | 370,000 addresses (UNI) | 95,000 addresses (MKR) | 161,000 addresses (AAVE) | As of May 2023 |
| | | Number of transactions by governor token holder address | Incoming: 2,137,000 TRX<br>Outgoing: 2,105,000 TRX | Incoming: 1,139,000 TRX<br>Outgoing: 1,121,000 TRX | Incoming: 966,000 TRX<br>Outgoing: 1,020,000 TRX | |
| | Degree of concentration on specific Oracle services | Oracle Service usage trends by DeFi | Provide oracle functionality within the project (TWAP: Time Weighted Average Price) | Provide oracle functionality within the project (oracle price feed) | Use of external oracle services (Chainlink) | As of April 2023 |
| | Lending Protocol related data | Collateral ratios based on collateral type | - | 19 types<br>102% to 5,000% | 10 types<br>125% to 200% | As of April 2023 |
| | | Leverage ratio (Leverage ratio = total debt/total assets) | - | 6 types of tokens<br>96.6% to 99.9% | 14 types of tokens<br>0.4% to 77.9% | As of April 2023 |

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-6. DeFi Related

(1) DeFi related

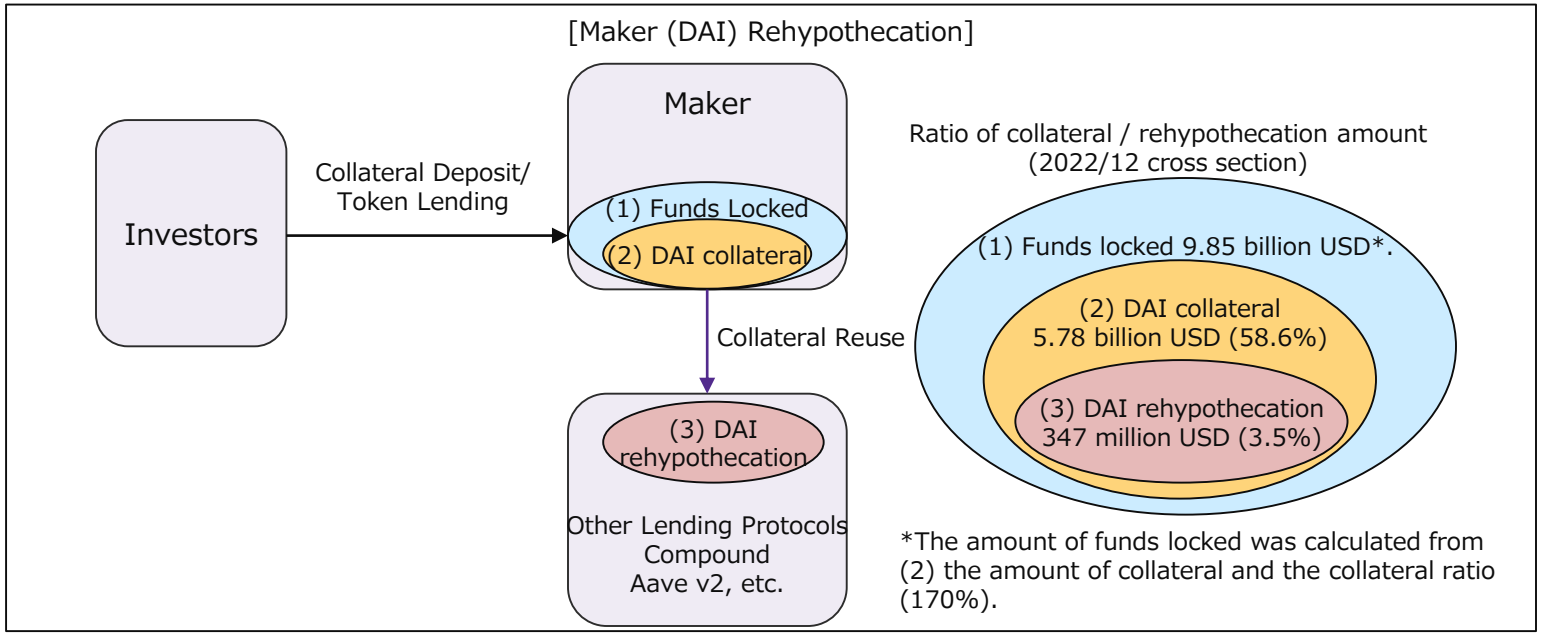
Table 4-3-6-1 Results of DeFi data survey (2/2)

<table>
<tr><th>Category</th><th>Surveyed Items</th><th>Surveyed Data</th><th>Data Survey Results (on-chain/off-chain)</th><th>Remarks</th></tr>
<tr><td rowspan="8">DeFi Related</td><td rowspan="3">Actual usage of cross-chain bridges (total amount of tokens locked, transactional relationships with VASPs, etc.)</td><td>Cross-chain bridge address</td><td>18 addresses</td><td rowspan="3">[Main Cross-Chain Bridges] As of 2023/4<table><tr><th>Cross-chain bridge</th><th>Total amount of tokens locked</th></tr><tr><td>Polygon Bridges</td><td>3.30 billion USD</td></tr><tr><td>Arbitrum Bridges</td><td>2.29 billion USD</td></tr><tr><td>Avalanche Bridge</td><td>1.53 billion USD</td></tr><tr><td>Optimism Bridges</td><td>1.28 billion USD</td></tr><tr><td>Ronin Bridge</td><td>700 million USD</td></tr></table></td></tr>
<tr><td>Total amount of tokens locked</td><td>9.50 billion USD</td></tr>
<tr><td>Number of transactions with VASPs at the above address</td><td>10,270,000 addresses</td></tr>
<tr><td rowspan="2">Actual damage from DeFi-related hacking (total amount of damage, number of cases, etc.)</td><td>Identification of hacked DeFi</td><td>10 hacking incidents occurred</td><td>For accruals in 2022</td></tr>
<tr><td>Total amount of hacking</td><td>2.49 billion USD</td><td>For accruals in 2022</td></tr>
<tr><td rowspan="2">Actual linkages between the traditional financial sector and DeFi (e.g., the amount invested in traditional financial assets using tokens locked to smart contracts as collateral)</td><td>Addresses held by financial institutions</td><td>155 addresses</td><td>Information held by blockchain analytics company</td></tr>
<tr><td>Number of transactions linked to financial institutions and DeFi</td><td>13,252 transactions</td><td></td></tr>
<tr><td>Degree of concentration on specific oracle services</td><td>External oracle services and number of DeFi used</td><td>Chainlink: 263 projects<br>TWAP (provided by Uniswap): 78 projects<br>Chronicle: 2 projects</td><td></td></tr>
<tr><td>DEX-related data (e.g., liquidity of major token pairs, entities with close trading relationships with the DEX)</td><td>Liquidity of major token pairs</td><td>Major token pairs: 31 pairs<br>(Uniswap: WETH, USDC, USDT, DAI, MATIC, etc.)<br>Total TVL: 10.13 billion USD</td><td></td></tr>
</table>

(2) Rehypothecation (collateral diversion)

Table 4-3-6-2 DeFi (Rehypothecation) Data Survey Results

| Category | Surveyed Items | Surveyed Data | Blockchain analytics company research results | | | | |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Acquisition Method | Uniswap | Maker | Aave |
| DeFi Related | Lending Protocol Related Data | The reality of rehypothecation (collateral diversion) | Etherscan<br>Dune Analytics<br>In-house database | Obtain loan balances where collateral from the surveyed lending protocols ware reused by other lending protocols<br>(as of 2022/12)<br>*Only tokens issued by own project are eligible (DAI/AAVE) | (Not applicable) | Total: 347 million USD<br>【Breakdown】<br>Compound<br>257 million USD<br>Aave v2<br>78 million USD<br>Aave v1<br>4.7 million USD, etc. | Total: 163,081 USD<br>【Breakdown】<br>Maker 147,935 USD<br>Euler Finance<br>14,611 USD, etc. |




*Rehypothecation amount is the value of the 2022/12 cross section

| Maker (DAI token) | | Aave (AAVE token) | |
|---|---|---|---|
| Rehypothecation Lender | Amount USD | Rehypothecation Lender | Amount USD |
| Compound | 256,862,012 | Maker | 147,935 |
| Aave v2 | 77,652,885 | Euler Finance | 14,611 |
| Aave v1 | 4,748,882 | Idle Cash | 535 |
| Euler Finance | 3,807,531 | Total amount | 163,081 |
| DyDx | 1,613,278 | | |
| Cream Finance | 1,401,051 | | |
| Yearn Finance | 662,674 | | |
| Idle Cash | 70,541 | | |
| Total amount | 346,818,854 | | |

Source: Dai Stats https://daistats.com/#/

# 4-3. Results of Financial Stability-Related Data Analysis
## 4-3-7. Main Findings

Table 4-3-7 Main Findings

| Main Findings | Contents |
|---|---|
| A certain amount of data is available that may be useful in assessing financial stability impacts. | • It is believed that a certain amount of data that could serve as a starting point for further risk analysis and evaluation could be presented in this initial data analysis, including the transaction relationships among entities such as VASPs and the actual situation of rehypothecation in DeFi.<br>• Regarding the availability of data as indicated in the FSB report, it was confirmed that in some cases data that the FSB indicated were available were difficult to obtain for this study, while in other cases data that the FSB indicated were not available were considered to be available for this study (but some data were limited). |
| The need for analysis using multiple data sources and the effectiveness of expert research | • The type of data that can be obtained and its reliability varies depending on the data source. For example, BC Explorer can obtain data on transactions and balances on the blockchain, but token prices are difficult to obtain. On the other hand, crypto asset-related databases can obtain market data such as crypto asset prices, but transactions on the blockchain are difficult to obtain. Blockchain analysis tools are mainly designed to collect information on high-risk VASPs and trace high-risk transactions, making it difficult to obtain some data related to stablecoin and DeFi (other analysis tools may be able to obtain data related to stablecoin and DeFi).<br>• It was confirmed that many survey items for which it is difficult to obtain data with analytical tools can be obtained with expert research (but only some data are limited).<br>• Where there are data sources other than those utilized in this study, such as data obtained through supervisory responses, it may be necessary for the financial authorities to ensure accessibility to multiple data sources and to monitor implications for financial stability. |
| Data contributing to the analysis of interconnectedness with the existing financial system is difficult to obtain | • In terms of the exposure of financial institutions and the actual status of payment use, not much data was available from the survey results. As a background, it is considered that off-chain data (e.g., information on custodians to whom financial institutions entrust digital assets, transaction and price data for payment use in e-commerce, etc.), which is difficult to obtain from public information, is necessary to grasp the actual status of these transactions. It is possible that many of these data are not currently held by blockchain analytics companies.<br>• On the other hand, there is a possibility that data can be obtained through supervisory measures (such as requesting reports from financial institutions) (which were not the subject of this survey), and it would be desirable for the authorities to explore various methods to strengthen monitoring capabilities. |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-1. Availability of Data as Indicated by the FATF Report

- With regard to the points raised in the FATF report, the results of an investigation into the possibility of data obtaining using various tools and expert research confirmed that, among the data examined in this research, some data, such as conversion to legal tender and crypto asset ATMs/kiosks, are difficult to obtain, but a certain amount of data that could potentially be obtained.
- Note that the results of this survey are only localized based on the analytical tools used in this research and the results of expert research.

(1) VASP data availability

〇: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-4-1-1 Data availability for VASP (1/3)

| Category | Surveyed Items | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | BC Explorer | Crypto Asset Related database | Blockchain analytics tools | Research by experts | |
| VASP | Investigation of transaction trends of relevant wallet addresses of major VASPs (including understanding of actual management conditions such as centralized/decentralized management and intra-group transactions) | Intra-group addresses held by major VASPs | △<br>A certain number of addresses identified as VASPs can be obtained. | ×<br>Difficult to obtain data | △<br>A certain number of addresses identified as VASPs can be obtained. | △<br>A certain number of addresses identified as VASPs can be obtained. | Targets are addresses identified as VASP by blockchain analytics companies |
| | | Number of transactions and value of transactions at the above addresses | △<br>Transaction data for each VASP and identified address can be obtained for each transaction (aggregation is difficult) | ×<br>Difficult to obtain data | △<br>Transaction data for each VASP and identified address can be obtained for each transaction (aggregation is difficult) | △<br>A certain number of transaction data for VASP and identified addresses can be obtained. | |
| | Major VASPs and related entities (institutional investors, financial institutions, etc.) and their actual transactions | Addresses of institutional investors and financial institutions | ▲<br>Limited to some addresses such as identified by account name, etc. | ×<br>Difficult to obtain data | ▲<br>Limited to some addresses such as identified by account name, etc. | ▲<br>Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as institutional investors, etc. by blockchain analytics companies |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-1. Availability of Data as Indicated by the FATF Report

(1) VASP data availability

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-4-1-1 Data availability for VASP (2/3)

| Category | Surveyed Items | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | BC Explorer | Crypto Asset Related database | Blockchain analytics tools | Research by experts | |
| VASP | Actual transactions between VASP-DeFi/unhosted wallets | DeFi Address | △<br>A certain number of addresses identified with DeFi can be obtained. | ×<br>Difficult to obtain data | △<br>A certain number of addresses identified with DeFi can be obtained. | △<br>A certain number of addresses identified with DeFi can be obtained. | Targets are addresses identified as DeFi or unhosted wallets by blockchain analytics companies |
| | | Unhosted Wallet Address | ▲<br>Limited to some addresses such as identified by account name, etc. | ×<br>Difficult to obtain data | ▲<br>Limited to some addresses such as identified by account name, etc. | ▲<br>Limited to some addresses such as identified by account name, etc. | |
| | | Number of transactions and value of transactions at the above addresses | △<br>Transaction data for DeFi and unhosted wallets and identified addresses can be obtained around one transaction (difficult to aggregate). | ×<br>Difficult to obtain data | △<br>Transaction data for DeFi and unhosted wallets and identified addresses can be obtained around one transaction (difficult to aggregate). | △<br>A certain number of transaction data for DeFi and unhosted wallets and identified addresses can be obtained. | |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-1. Availability of Data as Indicated by the FATF Report

(1) VASP data availability

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-4-1-1 Data availability for VASP (3/3)

| Category | Surveyed Items | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | BC Explorer | Crypto Asset Related database | Blockchain analytics tools | Research by experts | |
| VASP | Identification of VASP-related wallet addresses/transactions considered high risk | Addresses determined to be high risk (e.g., addresses used for criminal activity in the past) | × Difficult to obtain data | × Difficult to obtain data | △ A certain number of high risk addresses identified as VASPs can be obtained. | △ A certain number of high risk addresses identified as VASPs can be obtained. | Targets are addresses deemed high risk by blockchain analytics companies |
| | | Number of transactions and value of transactions at the above addresses | × Difficult to obtain data | × Difficult to obtain data | △ Transaction data for each VASP and identified address can be obtained for each transaction (aggregation is difficult) | △ A certain number of transaction data for VASP and identified addresses can be obtained. | |
| | Trends by location/region of VASPs (located in jurisdictions with no registration or inadequate regulatory requirements) | Address of unregistered VASP | × Difficult to obtain data | × Difficult to obtain data | ▲ A certain number of addresses identified as VASPs can be obtained. Difficult to search for unregistered VASPs | △ A certain number of addresses identified as VASPs can be obtained. | Rely on VASP registration information held by blockchain analytics companies in their own databases |
| | | Trends in unregistered VASPs by location and region | × Difficult to obtain data | × Difficult to obtain data | △ A certain number of identified VASP locations can be obtained. | △ A certain number of identified VASP locations can be obtained. | |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-1. Availability of Data as Indicated by the FATF Report

(2) Possibility of obtaining data from unhosted wallets

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-4-1-2 Data availability for Unhosted Wallets

| Category | Surveyed Items | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | BC Explorer | Crypto Asset Related database | Blockchain analytics tools | Research by experts | |
| Unhosted Wallet (incl. P2P) | P2P Transaction Facts | Unhosted Wallet Address | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as unhosted wallets by blockchain analytics companies |
| | | Number of transactions and value of total P2P transactions | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | |
| | | Percentage of Fraudulent Transactions | × Difficult to obtain data | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | |
| | Actual use of PET (e.g., mixing services) | Number of transactions and value of transactions for mixing services | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | ▲ Limited to some addresses such as identified by account name, etc. | ▲ Limited to some addresses such as identified by account name, etc. | Targets are addresses identified as mixing services by blockchain analytics companies |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-1. Availability of Data as Indicated by the FATF Report

(3) AML/CFT related data availability

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-4-1-3 Data availability for AML/CFT (1/2)

| Category | Surveyed Items | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | BC Explorer | Crypto Asset Related database | Blockchain analytics tools | Research by experts | |
| AML/CFT related | When converting large amounts of legal tender into large amounts of crypto assets | Addresses of users (accounts) that exchange crypto assets and legal tender | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | Legal tender exchange is mainly done by VASPs, with the possibility of data acquisition by supervisory authorities |
| | crypto assets identified as holding stolen funds or receive funds that are suspected to have been in the event | Addresses that are being misused | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | △ A certain number of target addresses can be obtained (each address can be obtained, but aggregation is difficult) | △ A certain number of target addresses can be obtained. | Targets are addresses identified as abusive by blockchain analytics companies |
| | | Address of the counterparty to the above address | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | △ A certain number of target addresses can be obtained (each address can be obtained, but aggregation is difficult) | △ A certain number of target addresses can be obtained. | |
| | Transferring funds from a VASP with no or inadequate customer relationship management (CDD) or identity verification (KYC) processes | Identification of VASPs that appear to have no CDD/KYC process at the time of joining the VASP | × Difficult to obtain data | × Difficult to obtain data | △ A certain number of VASPs can be obtained, but it is difficult to search | △ The VASP for the relevant condition is a certain number can be obtained | Rely on VASP registration information held by blockchain analytics companies in their own databases |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-1. Availability of Data as Indicated by the FATF Report

(3) AML/CFT related data availability

○: All data can be obtained
△: Data generally obtainable, but some difficult to obtain
▲: Some data can be obtained, but only to a limited extent
×: No data can be obtained at all
-: Not included in this survey

Table 4-4-1-3 Data availability for AML/CFT (1/2)

| Category | Surveyed Items | Surveyed Data | Results of availability of data | | | | Remarks |
|---|---|---|---|---|---|---|---|
| | | | BC Explorer | Crypto Asset Related database | Blockchain analytics tools | Research by experts | |
| AML/CFT related | Use of crypto asset ATMs/kiosks in locations with a high risk of increased criminal activity | Addresses using crypto asset ATM/kiosk | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | × Difficult to obtain data | Difficult to obtain data on crypto assets ATM/kiosk |
| | Transactions at crypto asset addresses associated with fraud and extortion, ransomware schemes, sanctioned addresses, darknet marketplaces, or other illegal websites | Cryptographic asset addresses associated with illegal websites | ▲ Limited to some addresses such as identified by account name, etc. | × Difficult to obtain data | △ A certain number of target addresses can be obtained (each address can be obtained, but aggregation is difficult) | △ A certain number of target addresses can be obtained. | Targets are addresses identified as fraudulent, extortion, etc. by blockchain analytics companies |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-2. Research Survey Items

- In this chapter, four survey items were researched by experts from a blockchain analytics company, setting specific survey items such as the number and amount of transactions and the actual use of suspicious transactions by category, such as VASPs and lending platform.
- The research results were organized into tables and graphs after organizing the data, and the trends and characteristics seen in the results were discussed.

Table 4-4-2 Research Survey Items

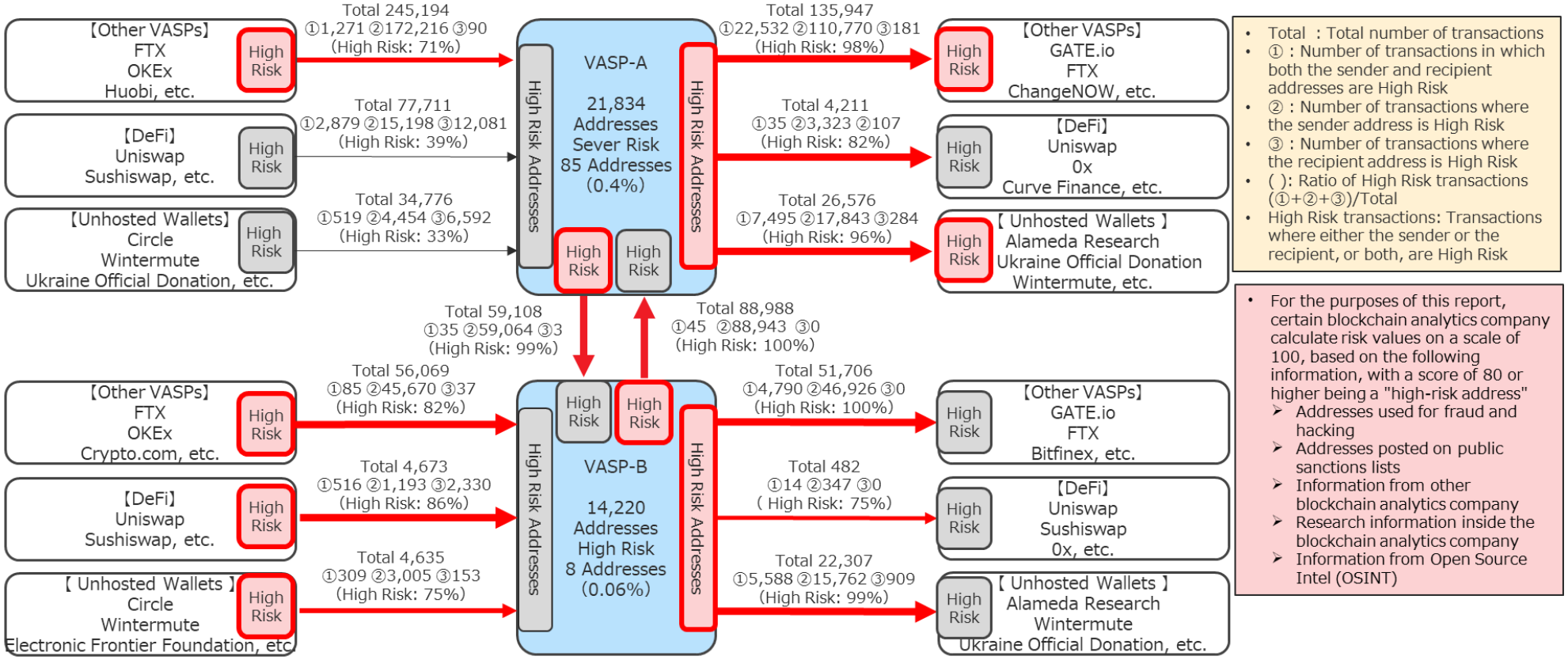
| Survey Items | Survey Contents | Supplement |
|---|---|---|
| Trends in high-risk transaction ratios for major VASPs | • The two main crypto asset traders were surveyed by category for the number of transactions, transaction value, and number of high-risk transactions in three categories: incoming, within their own company, and outgoing. | • Account category names and account names used classifications defined by the blockchain analytics companies.<br>• The transaction amount was calculated using the token price and other rates as of April 2023. |
| Trends in high-risk transaction ratios of major lending platform | • The number of transactions, value of transactions, and number of high-risk transactions by category were examined for one major lending platform in three categories: incoming, within their own company, and outgoing. | |
| Trends in high-risk Transaction Ratios for Unhosted Wallets | • The number of transactions, transaction value, and high-risk transactions for unhosted wallets were examined by category, by breakdown of DeFi among categories, and by token, for three categories: incoming, P2P (in unhosted wallets), and outgoing. | |
| AML/CFT related data | • The survey of suspicious transactions included small-value transactions, consecutive high-value transactions, mixing services, fraudulent/extortion and sanctioned addresses, online gambling services, and other high-risk addresses.<br>• The location and regional trends of unregistered VASPs that are not registered in the jurisdiction in which they are located were investigated. | |

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-3. Major VASPs

(1) Major VASPs: Summary of high-risk transactions for VASP-A/VASP-B

- High-risk transactions are mainly remittance from VASP-A/VASP-B and other VASPs (token transfers from high-risk addresses managed by VASPs), all of which account for more than 70% of the total.
  - ➢ However, under the definition of high-risk addresses and transactions, many VASP-related transactions are considered to be classified as "high-risk" (i.e., a large number of transactions are sent and received at a small number of addresses managed by the VASP).
  - ➢ The actual situation of the addresses (which are likely to be classified as high-risk) and whether they reflect the actual situation requires close examination (details are provided on the next page and beyond).
- A significant number of high-risk transactions with DeFi and unhosted wallets (including some large operators and funds) were also identified.

Figure 4-4-3-1 Summary of major VASPs high-risk transactions



# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-3. Major VASPs (VASP-A)

(2) Major VASPs: VASP-A By Category

Figure 4-4-3-2 VASP-A number of transactions / amount by category

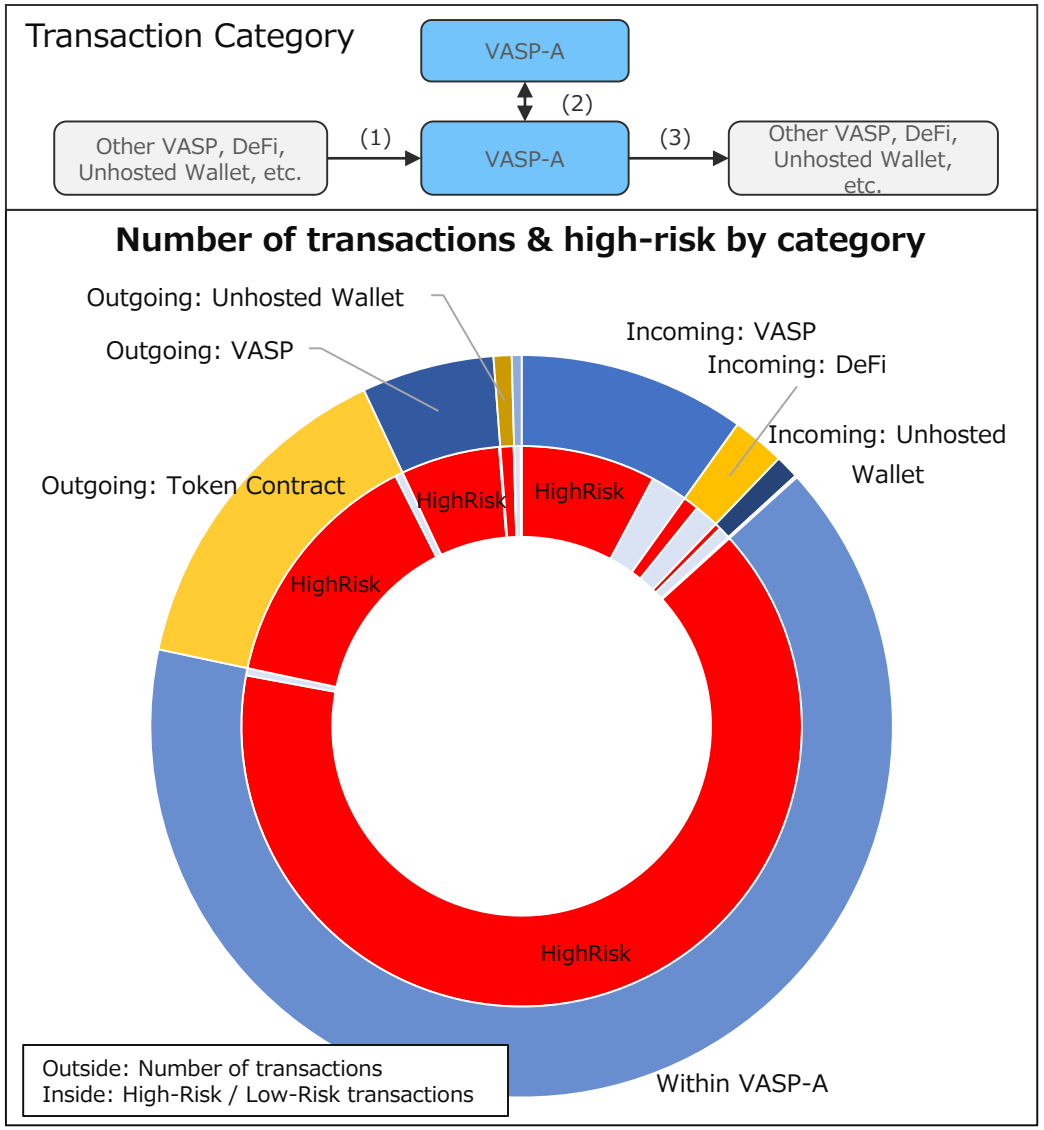



Table 4-4-3-2 VASP-A transactions / amount data by category

| Transaction Category | Account Category | Number of transactions | | Number of high-risk transactions | | Amount of transaction | |
|---|---|---|---|---|---|---|---|
| | | Transactions | Transactions Ratio | High-risk transactions | High Risk Ratio | Amount M$ | Amount Ratio |
| (1) Incoming | VASP | 334,182 | 74.3% | 262,565 | 78.6% | 51,239 | 77.8% |
| | DeFi | 77,711 | 17.3% | 30,158 | 38.8% | 528 | 0.8% |
| | Unhosted Wallet | 34,776 | 7.7% | 11,565 | 33.3% | 13,791 | 20.9% |
| | Token Contract | 2,320 | 0.5% | 1,864 | 80.3% | 27 | 0.0% |
| | Bridge | 566 | 0.1% | 146 | 25.8% | 148 | 0.2% |
| | Other | 133 | 0.0% | 42 | 31.6% | 123 | 0.2% |
| | Total | 449,688 | 100.0% | 306,340 | 68.1% | 65,856 | 100.0% |
| (2) Within VASP-A | VASP | 2,198,665 | 100.0% | 2,184,570 | 99.4% | 625,406 | 100.0% |
| | Total | 2,198,665 | 100.0% | 2,184,570 | 99.4% | 625,406 | 100.0% |
| (3) Outgoing | VASP | 195,055 | 26.6% | 192,585 | 98.7% | 27,079 | 62.1% |
| | DeFi | 4,211 | 0.6% | 3,465 | 82.3% | 46 | 0.1% |
| | Unhosted Wallet | 26,576 | 3.6% | 25,622 | 96.4% | 15,873 | 36.4% |
| | Token Contract | 496,837 | 67.8% | 481,607 | 96.9% | 217 | 0.5% |
| | Bridge | 3,451 | 0.5% | 3,117 | 90.3% | 398 | 0.9% |
| | Other | 6,756 | 0.9% | 6,157 | 91.1% | 0 | 0.0% |
| | Total | 732,886 | 100.0% | 712,553 | 97.2% | 43,613 | 100.0% |

[Discussion]

- “(2) Within VASP-A” is the highest ratio within High-risk transactions.
  → Transactions within the VASP are concentrated in transfers to specific high-risk addresses (5 addresses).
  Some addresses with high transaction volume are determined to be "high risk" based on their track record of being used for fraud and crimes, and all transactions associated with such addresses may be classified as "high risk“.
  All transactions related to the address may be classified as "high risk" (in reality, the majority of transactions may not be problematic).
- Next higher ratio are “(3) Outgoing”, followed by “(1) Incoming”.
  → As “(2) Within VASP-A”, it is possible that the number of transactions to a particular high-risk address in VASP is high.

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-3. Major VASPs (VASP-B)

### (3) Major VASPs: VASP-B By Category

Figure 4-4-3-3 VASP-B number of transactions / amount by category

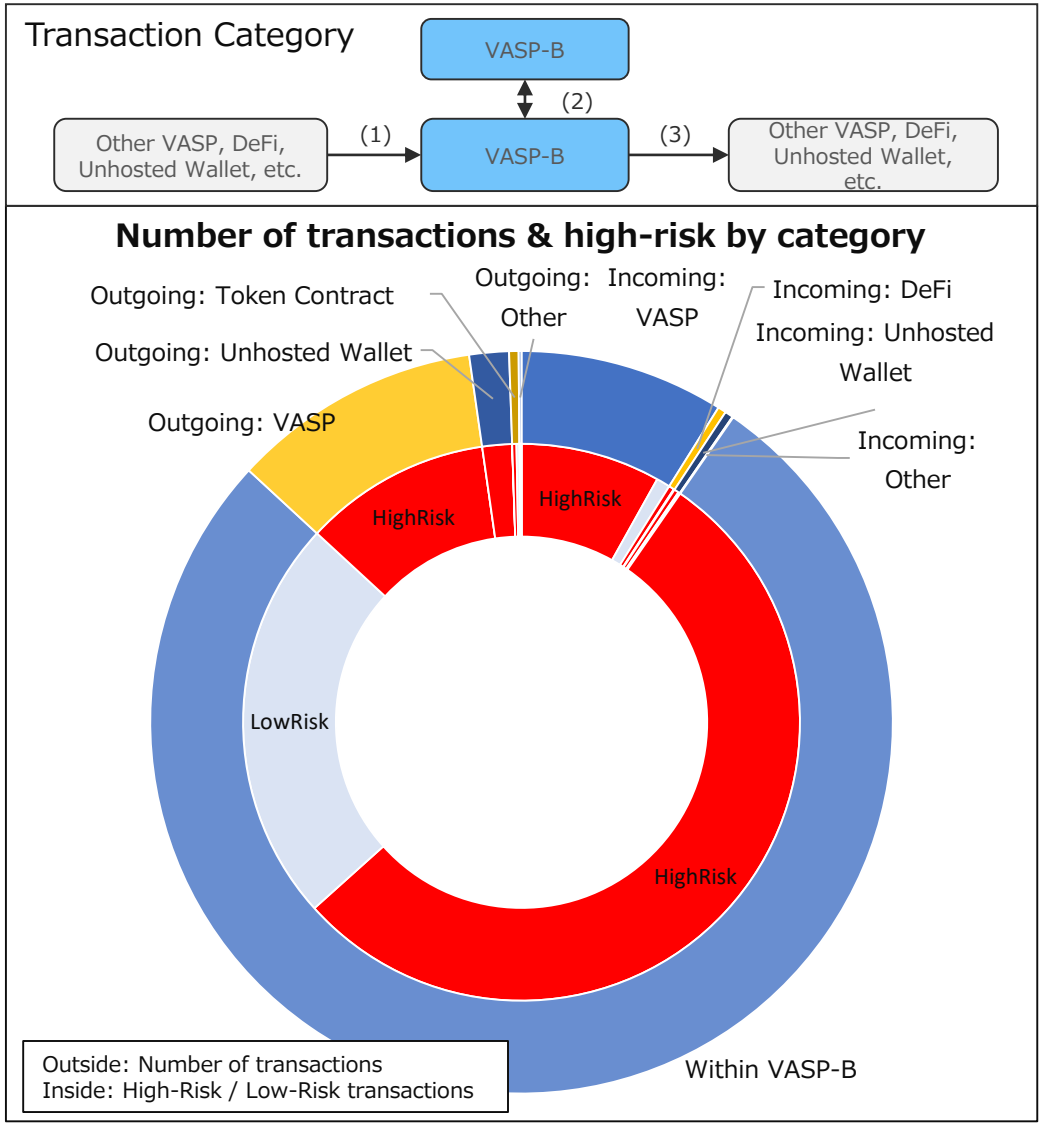



Table 4-4-3-3 VASP-B transactions / amount data by category

| Transaction Category | Account Category | Number of transactions | | Number of high-risk transactions | | Amount of transaction | |
|---|---|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | High-risk transactions | High Risk Ratio | Amount M$ | Amount Ratio |
| (1) Incoming | VASP | 115,177 | 92.1% | 104,894 | 91.1% | 17,190 | 20.6% |
| | DeFi | 4,673 | 3.7% | 4,039 | 86.4% | 123 | 0.1% |
| | Unhosted Wallet | 4,635 | 3.7% | 3,467 | 74.8% | 65,944 | 79.2% |
| | Token Contract | 306 | 0.2% | 304 | 99.3% | 0 | 0.0% |
| | Bridge | 192 | 0.2% | 30 | 15.6% | 1 | 0.0% |
| | Other | 6 | 0.0% | 6 | 100.0% | 0 | 0.0% |
| | Total | 124,989 | 100.0% | 112,740 | 90.2% | 83,259 | 100.0% |
| (2) Within VASP-B | VASP | 999,058 | 100.0% | 694,838 | 69.5% | 97,707 | 100.0% |
| | Total | 999,058 | 100.0% | 694,838 | 69.5% | 97,707 | 100.0% |
| (3) Outgoing | VASP | 140,704 | 82.8% | 140,704 | 100.0% | 13,655 | 64.9% |
| | DeFi | 482 | 0.3% | 361 | 74.9% | 2,583 | 12.3% |
| | Unhosted Wallet | 22,307 | 13.1% | 22,259 | 99.8% | 4,514 | 21.5% |
| | Token Contract | 5,320 | 3.1% | 3,179 | 59.8% | 1 | 0.0% |
| | Bridge | 1,072 | 0.6% | 1,072 | 100.0% | 279 | 1.3% |
| | Other | 51 | 0.0 | 34 | 66.7% | 0 | 0.0% |
| | Total | 169,936 | 100.0 | 167,609 | 98.6% | 21,032 | 100.0% |

[Discussion]

- High-risk transactions have the highest ratio of “(3) outgoing” within transaction categories.
  → “(3) Outgoing” may be due to the high number of transactions from certain high-risk addresses (8 addresses) in the VASP.
  It is possible that some addresses with high transaction volume are determined to be “high risk” based on their track record of being used for fraud and crime, and that all transactions associated with such addresses and all transactions related to the address may be classified as "high risk".
- Next, the ratios are high for “(1) Incoming” and “(2) Within VASP-B”.
  → As with “(3) Outgoing”, the number of transactions for certain high-risk addresses in VASP may be high.

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-4. Major Lending Platform

### (1) Major Lending Platform: By Category

Figure 4-4-1 Lending Platform number of transactions / amount by category

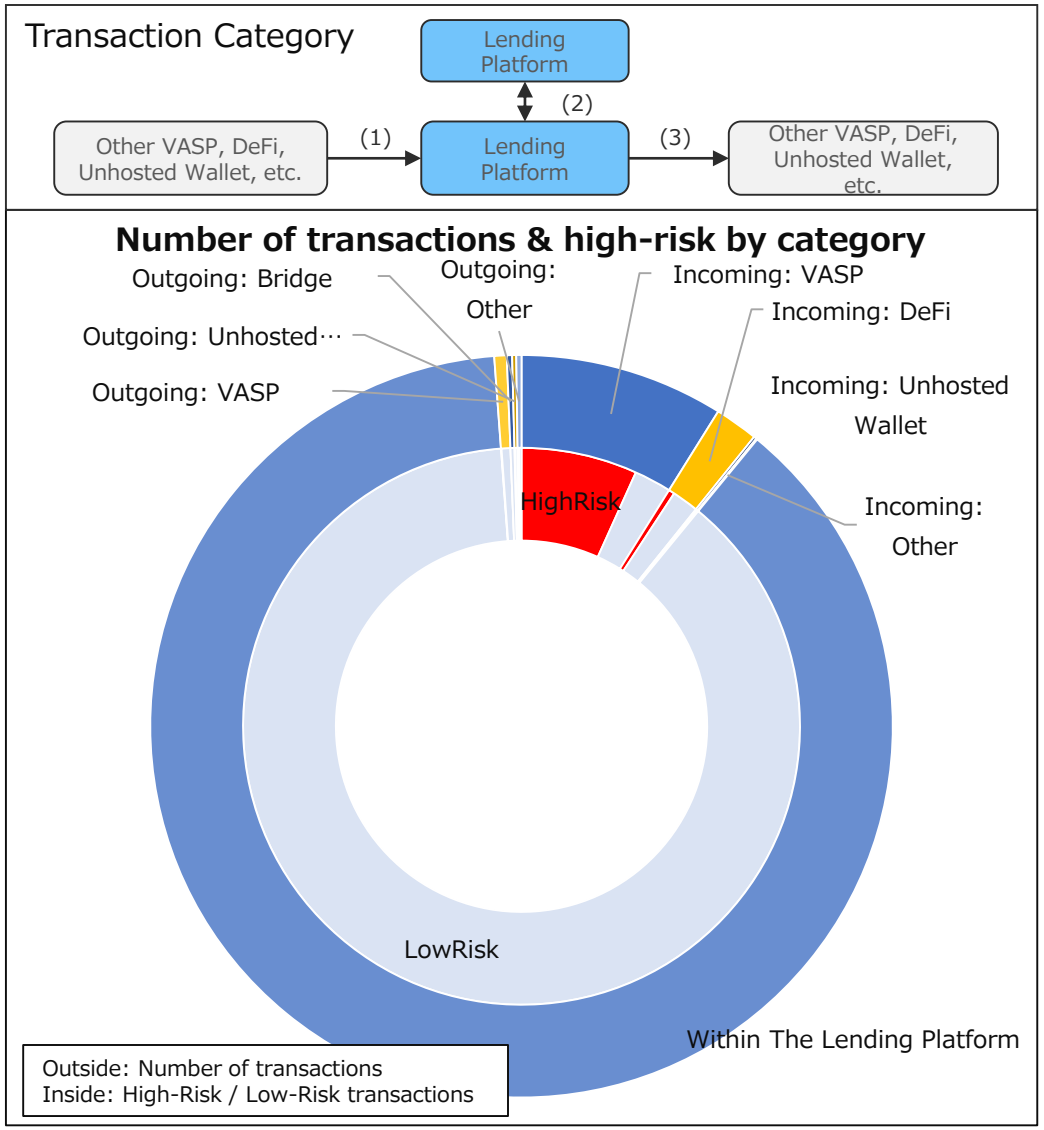



Table 4-4-1 Lending Platform transactions / amount data by category

| Transaction Category | Account Category | Number of transactions | | Number of high-risk transactions | | Amount of transaction | |
|---|---|---|---|---|---|---|---|
| | | Transactions | Transaction ratio | High-risk transactions | High Risk Ratio | Amount M$ | Amount Ratio |
| (1) Incoming | VASP | 12,841 | 81.2% | 9,733 | 75.8% | 6,807 | 99.7% |
| | DeFi | 2,727 | 17.2% | 501 | 18.4% | 6 | 0.1% |
| | Unhosted Wallet | 174 | 1.1% | 146 | 83.9% | 15 | 0.2% |
| | Token Contract | 50 | 0.3% | 40 | 80.0% | 0 | 0.0% |
| | Bridge | 12 | 0.1% | 4 | 33.3% | 0 | 0.0% |
| | Other | 10 | 0.1% | 9 | 90.0% | 0 | 0.0% |
| | Total | 15,814 | 100.0% | 10,433 | 66.0% | 6,828 | 100.0% |
| (2) Within The Lending Platform | Lending Platform | 126,946 | 100.0 | 0 | 0.0% | 8,015 | 100.0% |
| | Total | 126,946 | 100.0 | 0 | 0.0% | 8,015 | 100.0% |
| (3) Outgoing | VASP | 782 | 46.1% | 40 | 5.1% | 177 | 43.0% |
| | DeFi | 0 | 0.0 | 0 | 0.0% | 0 | 0.0% |
| | Unhosted Wallet | 256 | 15.1% | 62 | 24.2% | 141 | 34.2% |
| | Token Contract | 224 | 13.2% | 125 | 55.8% | 0 | 0.0% |
| | Bridge | 332 | 19.6% | 0 | 0.0% | 21 | 5.1% |
| | Other | 103 | 6.1% | 4 | 3.9% | 73 | 17.6% |
| | Total | 1,697 | 100.0 | 231 | 13.6% | 412 | 100.0% |

[Discussion]

- High risk transactions have the highest ratio of “(1) Incoming”. By category, other VASPs, unhosted wallets, and token contracts have the high ratios.
  → For VASPs and token contracts, addresses with a high number of transactions may be more likely to be used for fraud and crime. For unhosted wallets, is it possible that many transfers are made from specific high-risk addresses?
- There is no high-risk transactions of “(2) Within The Lending Platform”.
  → The number of transactions at the Lending Platform's address is smaller than that of VASPs, etc., which may make it less likely to be used for fraud or crime.

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-5. Unhosted Wallets

*MEV (Maximum Extractable Value) BOT:.
Automated execution software that analyzes the waiting transaction pool (mempool) of the Ethereum blockchain and obtains value by front running, etc.

### (1) Unhosted Wallets: By Category

Figure 4-4-5-1 Unhosted Wallets number of transactions / amount by category

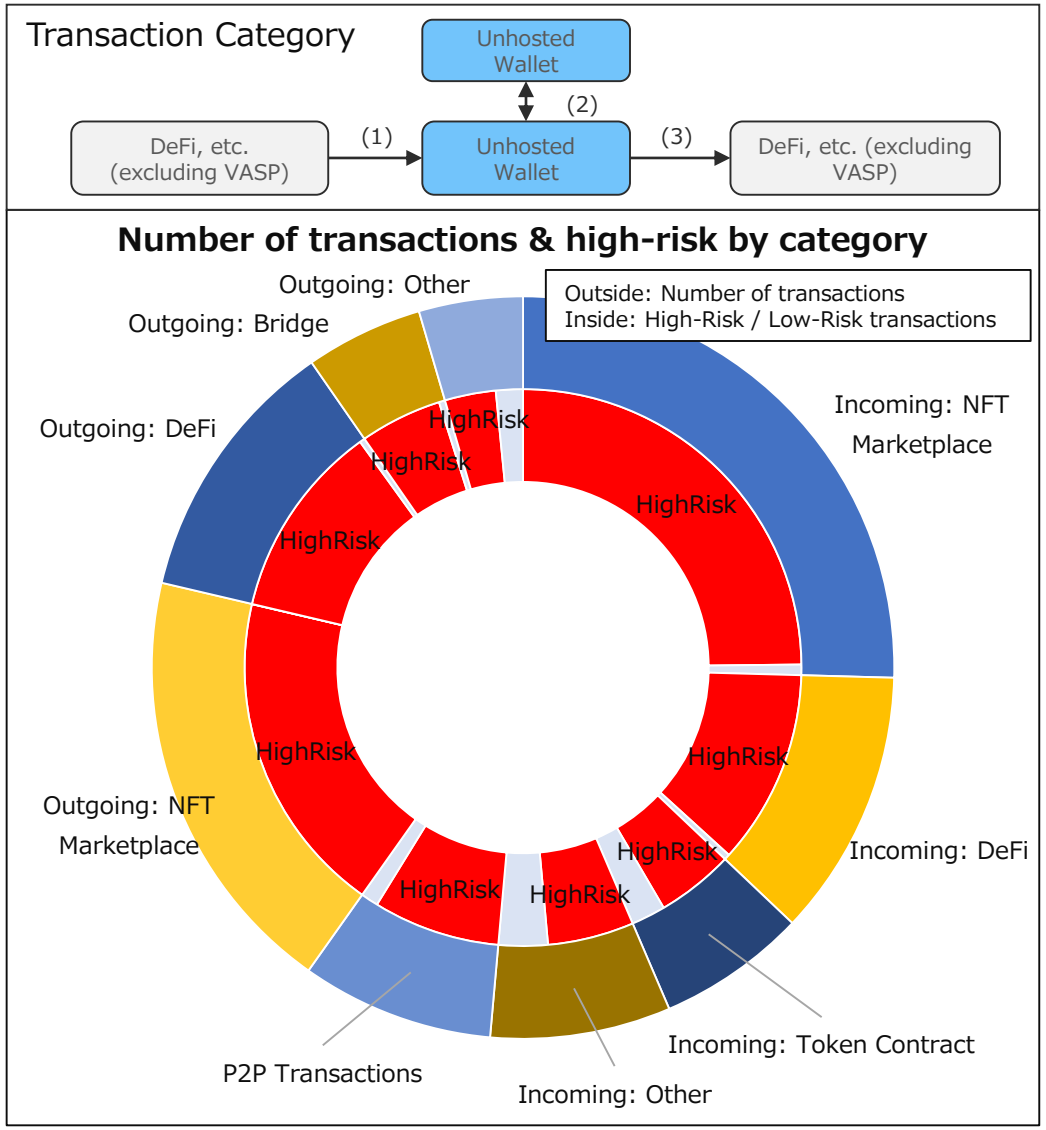



Table 4-4-5-1 Unhosted Wallets transactions / amount data by category

| Transaction Category | Account Category | Addresses | Number of transactions | | Number of high-risk transactions | | Amount of transaction | |
|---|---|---|---|---|---|---|---|---|
| | | | Transactions | Transaction ratio | High-risk transactions | High Risk Ratio | Amount M$ | Amount Ratio |
| (1) Incoming | NFT Marketplace | 190 | 1,468,421 | 49.5% | 1,433,197 | 97.6% | 152 | 0.2% |
| | DeFi | 8,752 | 672,335 | 22.7% | 653,168 | 97.1% | 30,537 | 44.9% |
| | Token Contract | 1,753 | 373,899 | 12.6% | 259,006 | 69.3% | 22,378 | 32.9% |
| | Bridge | 895 | 271,589 | 9.1% | 265,744 | 97.8% | 10,179 | 15.0% |
| | MEV BOT* | 103 | 152,869 | 5.2% | 11,550 | 7.6% | 989 | 1.5% |
| | Other | 549 | 29,174 | 1.0% | 11,861 | 40.7% | 3,818 | 5.6% |
| | Total | 12,242 | 2,968,287 | 100.0% | 2,634,526 | 88.8% | 68,053 | 100.0% |
| (2) P2P Transactions | P2P Transactions | 5,989 | 484,394 | 100.0% | 425,882 | 87.9% | 28,967 | 100.0% |
| | Total | 5,989 | 484,394 | 100.0% | 425,882 | 87.9% | 28,967 | 100.0% |
| (3) Outgoing | NFT Marketplace | 77 | 1,088,944 | 46.9% | 1,088,322 | 99.9% | 1,083 | 2.1% |
| | DeFi | 4,799 | 674,524 | 29.1% | 656,787 | 97.4% | 22,876 | 44.0% |
| | Token Contract | 1,361 | 248,009 | 10.7% | 160,917 | 64.9% | 16,077 | 30.9% |
| | Bridge | 500 | 295,673 | 12.7% | 275,222 | 93.1% | 10,149 | 19.5% |
| | MEV BOT* | 27 | 3,963 | 0.2% | 2,834 | 71.5% | 344 | 0.7% |
| | Other | 329 | 9,179 | 0.4% | 7,087 | 77.2% | 1,498 | 2.9% |
| | Total | 7,093 | 2,320,292 | 100.0% | 2,191,169 | 94.4% | 52,027 | 100.0% |

[Discussion]

- High risk transactions have the highest ratio of "(3) Outgoing". By category, other VASPs, unhosted wallets, and bridges have high ratios.
  → VASPs and bridges may be more likely to be used for fraud and crime, as addresses with a high number of transactions are more likely to be used for fraud and crime.
  VASPs and bridges are likely to be used for fraud and crime.
  Unhosted wallets may have a high number of transactions of certain high-risk addresses?
- Next, the ratios are high for "(1) Incoming" and "(2) P2P transactions".
  → This is considered that the ratio of transactions of high-risk addresses is high, as is the case with "(3) Outgoing"?

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-5. Unhosted Wallets

(2) Unhosted Wallets: DeFi breakdown among Category

Figure 4-4-5-2 Unhosted Wallets number of transactions / amount by DeFi

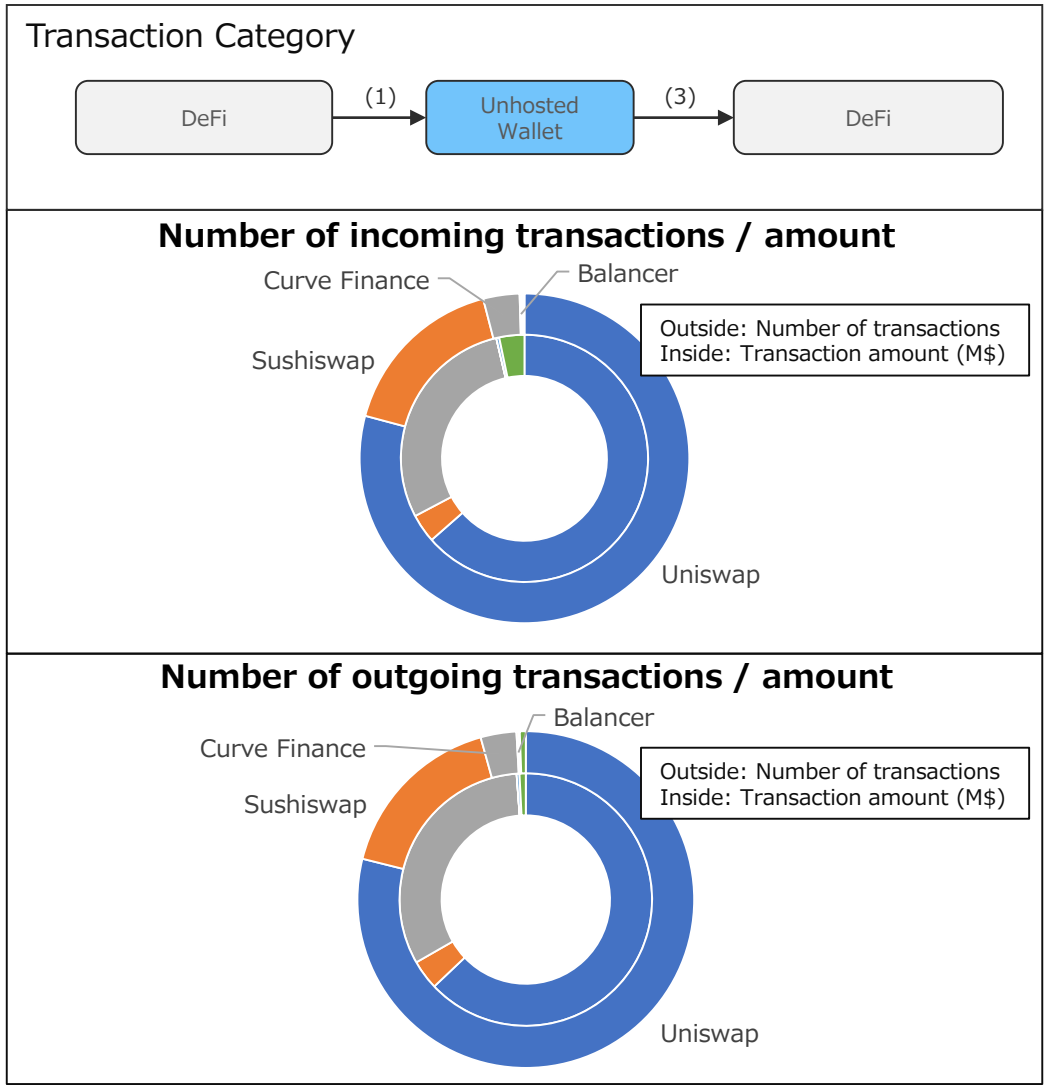



Table 4-4-5-2 Unhosted Wallets transactions / amount data by DeFi

| DeFi | Service | (1) Incoming | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|
| | | transactions | Transaction ratio | amount M$ | transactions | Transaction ratio | amount M$ |
| Uniswap | Decentralized Exchange | 532,196 | 79.2% | 19,400 | 532,203 | 78.9% | 14,393 |
| Sushiswap | Decentralized Exchange | 113,024 | 16.8% | 1,144 | 113,155 | 16.8% | 869 |
| Curve Finance | Decentralized Exchange | 23,941 | 3.6% | 8,874 | 23,170 | 3.4% | 7,348 |
| Balancer | Decentralized Exchange | 1,279 | 0.2% | 3 | 1,288 | 0.2% | 2 |
| mStable | Stablecoins Issuance | 897 | 0.1% | 114 | 837 | 0.1% | 81 |
| Other | - | 998 | 0.1% | 1,002 | 3,871 | 0.6% | 183 |
| Total | | 672,335 | 100.0% | 30,537 | 674,524 | 100.0 | 22,876 |

[Discussion]

- Both “(1) Incoming” and “(3) Outgoing” have a large number of transactions on decentralized exchanges.
  → Likely to exchange of crypto assets, liquidity provision, and remittance of staking.
- Of the decentralized exchanges, Uniswap has a large number of transactions for both “(1) Incoming” and “(3) Outgoing”.
  → Uniswap is considered a multi-type token exchange (approx. 700 types)
- The number of transactions “(1) Incoming” and “(3) Outgoing” is almost the same for each DeFi.
  → Details need to be scrutinized, but for example, is there a possible movement to transfer tokens exchanged on decentralized exchanges to unhosted wallets?

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-5. Unhosted Wallets

(3) Unhosted Wallets: By Token

Figure 4-4-5-3 Unhosted Wallets number of transactions / amount by Token

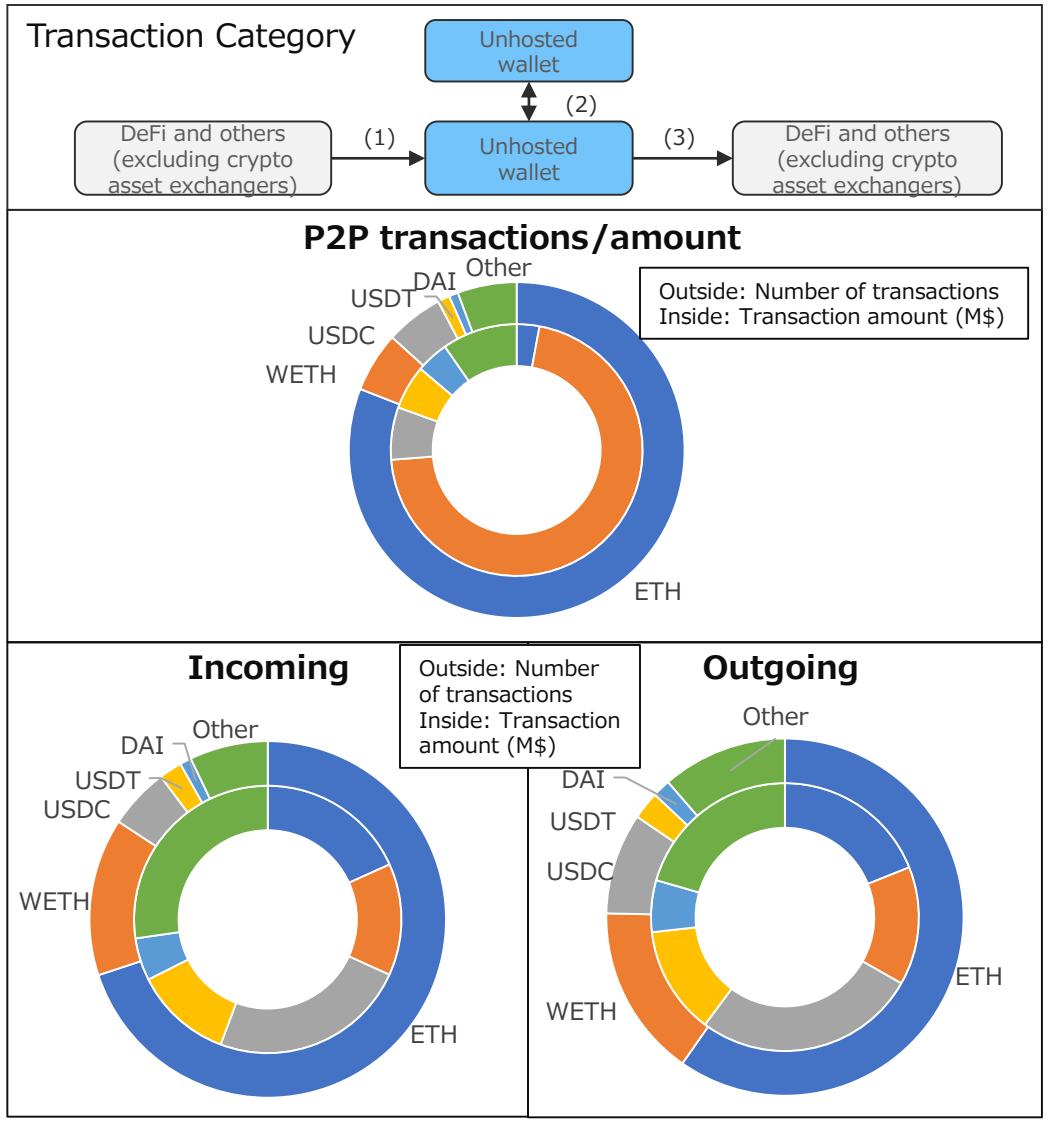



Table 4-4-5-3 Unhosted Wallets transactions / amount data by Token

| Token | Classification | (1) Incoming | | | (2) P2P Transactions | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | transactions | Transaction ratio | amount M$ | transactions | Transaction ratio | amount M$ | transactions | Transaction ratio | amount M$ |
| ETH | Native token | 2,076,058 | 69.9% | 12,420 | 391,975 | 80.9% | 843 | 1,386,001 | 59.7% | 9,853 |
| WETH | Native token | 424,295 | 14.3% | 9,219 | 28,025 | 5.8% | 20,524 | 362,035 | 15.6% | 7,439 |
| USDC | Stablecoins | 164,494 | 5.5% | 16,299 | 26,908 | 5.6% | 1,952 | 212,593 | 9.2% | 14,020 |
| USDT | Stablecoins | 61,740 | 2.1% | 8,053 | 5,655 | 1.2% | 1,642 | 58,577 | 2.5% | 6,769 |
| DAI | Stablecoins | 30,959 | 1.0% | 3,503 | 4,241 | 0.9% | 1,209 | 37,793 | 1.6% | 3,255 |
| Other | - | 210,741 | 7.1% | 18,559 | 27,590 | 5.7% | 2,797 | 263,293 | 11.3% | 10,691 |
| Total | | 2,968,287 | 100.0% | 68,053 | 484,394 | 100.0% | 28,967 | 2,320,292 | 100.0% | 52,027 |

*The number of transactions for about 800 types of tokens in "Other" for "(1) Incoming" and about 700 types of tokens in "Other" for "(3) Outgoing.

[Discussion]

- ETH and WETH (tokens pegged 1:1 to ETH) has large number of transactions in all transaction categories.
  Next, there are many transactions of stablecoins such as USDC, USDT, DAI, etc.
  → This is considered to be due to their use in exchanges with other tokens (e.g. to fix the amount of money)
- WETH is not among the major VASPs or lending platform in terms of number and amount of transactions, but has a high number and amount of transactions in the unhosted wallet.
  → WETH is an ERC-20 compliant token to facilitate the use of ETH for DeFi, NFT services, etc., and this is thought to be due to its high use by DeFi, etc.

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-6. AML/CFT Related

(1) Number of addresses associated with holders of stolen funds

Figure 4-4-6-1 Stolen funds number of addresses by category

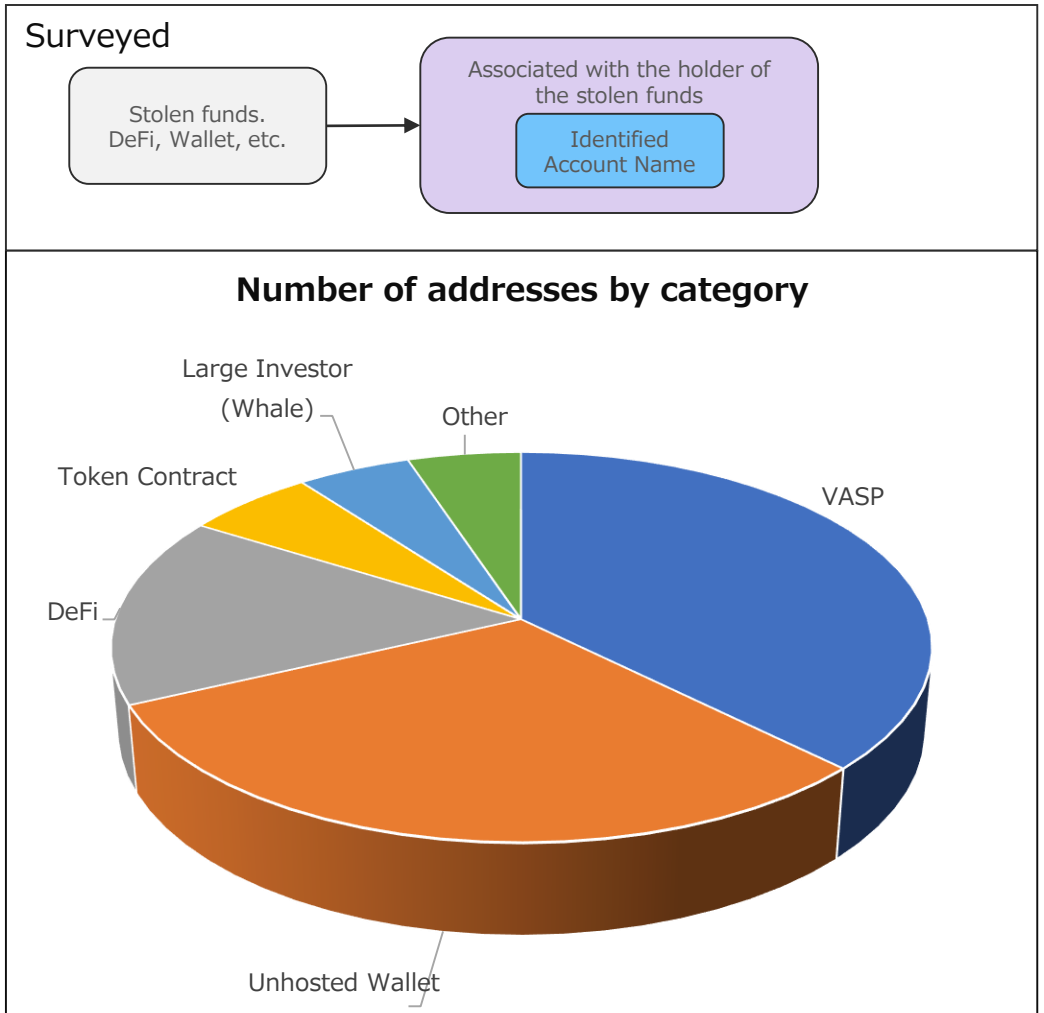



Table 4-4-6-1 Stolen Funds addresses data by category

| Category | Addresses | Ratio |
|---|---|---|
| VASP | 1,567 | 37.4% |
| Unhosted Wallet | 1,285 | 30.7% |
| DeFi | 662 | 15.8% |
| Token Contract | 246 | 5.9% |
| Large Investor (Whale) | 216 | 5.2% |
| Other | 215 | 5.1% |
| Total | 4,191 | 100.0 |

| Identification of address holder | Addresses | Ratio |
|---|---|---|
| Identified address holders | 4,191 | 2.6% |
| Unknown address holders | 158,918 | 97.4% |
| Total | 163,109 | 100.0% |

[Discussion]

- Of the addresses associated with the holders of the stolen funds, only 3% of all addresses were able to identify the account names.
  → Even if the addresses could be identified by the databases of blockchain analytics company, most of the account names could not be identified, suggesting that it is extremely difficult to identify accounts from off-chain information and other sources.
- Regarding the addresses that were identified, VASP addresses are the highest ratio. Unhosted wallets were next higher ratio.
  → It is possible that VASP and Unhosted Wallet have many addresses that were used for crimes and frauds in the past. However, since VASPs are considered to be relatively easy to identify, this may not necessarily indicate an overall trend.

*"Addresses associated with holders of stolen funds" used data on known attackers held by a blockchain analytics company.

(2) Number of addresses using mixing services

Figure 4-4-6-2 Mixing services number of addresses by category

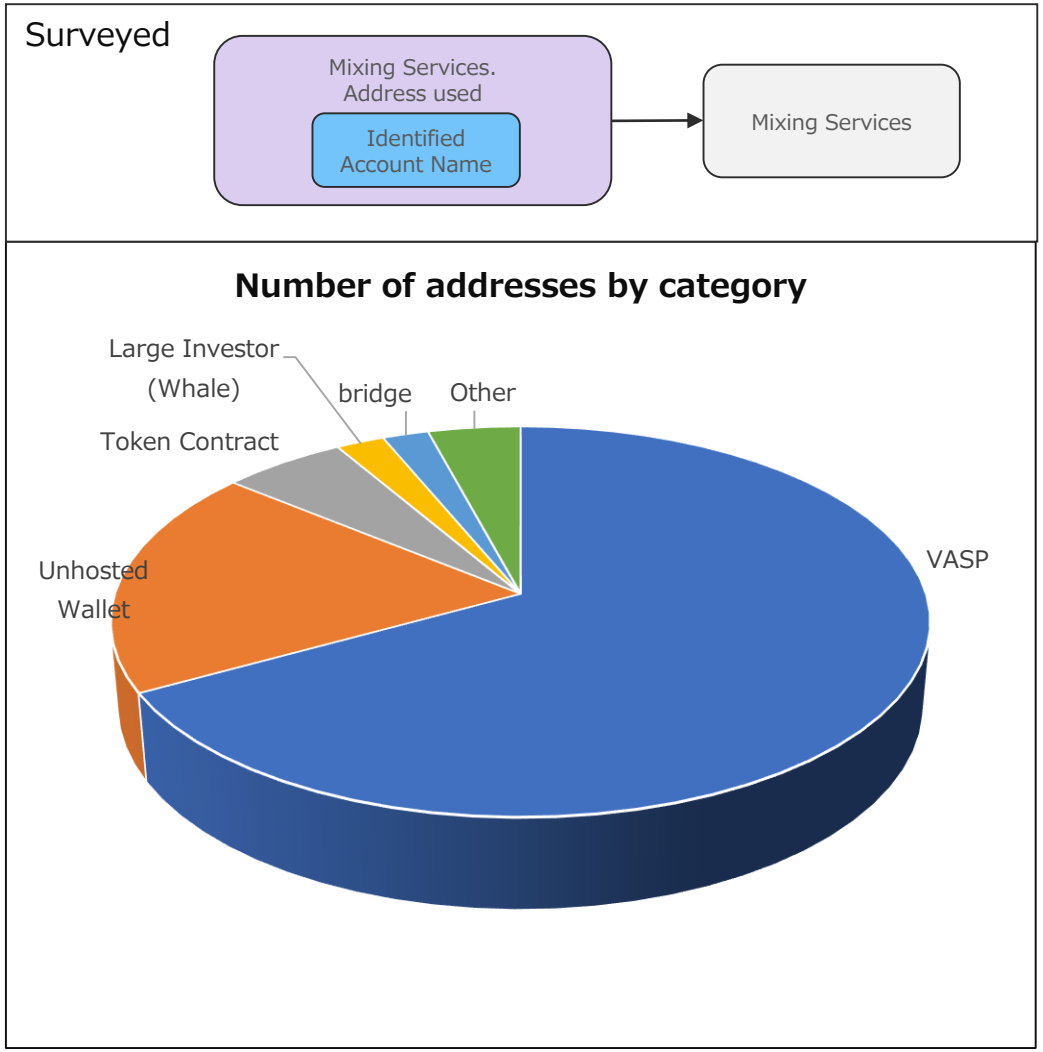



Table 4-4-6-2 Mixing services addresses data by category

| Category | Addresses | Ratio |
|---|---|---|
| VASP | 22,257 | 67.0% |
| Unhosted Wallet | 6,304 | 19.0% |
| Token Contract | 1,866 | 5.6% |
| Large investor (Whale) | 727 | 2.2% |
| Bridge | 692 | 2.1% |
| Other | 1,390 | 4.2% |
| Total | 33,236 | 100.0% |

| Identification of address holder | Addresses | Ratio |
|---|---|---|
| Identified address holders | 33,236 | 0.4% |
| Unknown address holders. | 9,001,940 | 99.6% |
| Total | 9,035,176 | 100.0% |

[Discussion]

- The majority of mixing services related addresses identified were related to Tornado Cash.
- Of the addresses that used mixing services, account names could be identified for 0.4% of the total.
  → Even if the addresses that used the mixing service could be identified through the investigation of on-chain transaction information, most of the account names could not be identified, suggesting that it is extremely difficult to identify accounts from off-chain information and other sources.
- By category, VASP addresses are the highest ratio. Unhosted wallets are next higher ratio.
  → Possibility that VASP users or unhosted wallet owners are utilizing mixing services for some purpose (including ML).

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-6. AML/CFT Related

(3) Number of transactions and amount of addresses associated with fraud and extortion, ransomware, sanctioned addresses

Figure 4-4-6-3 Fraud, etc. number of transactions / amount by category

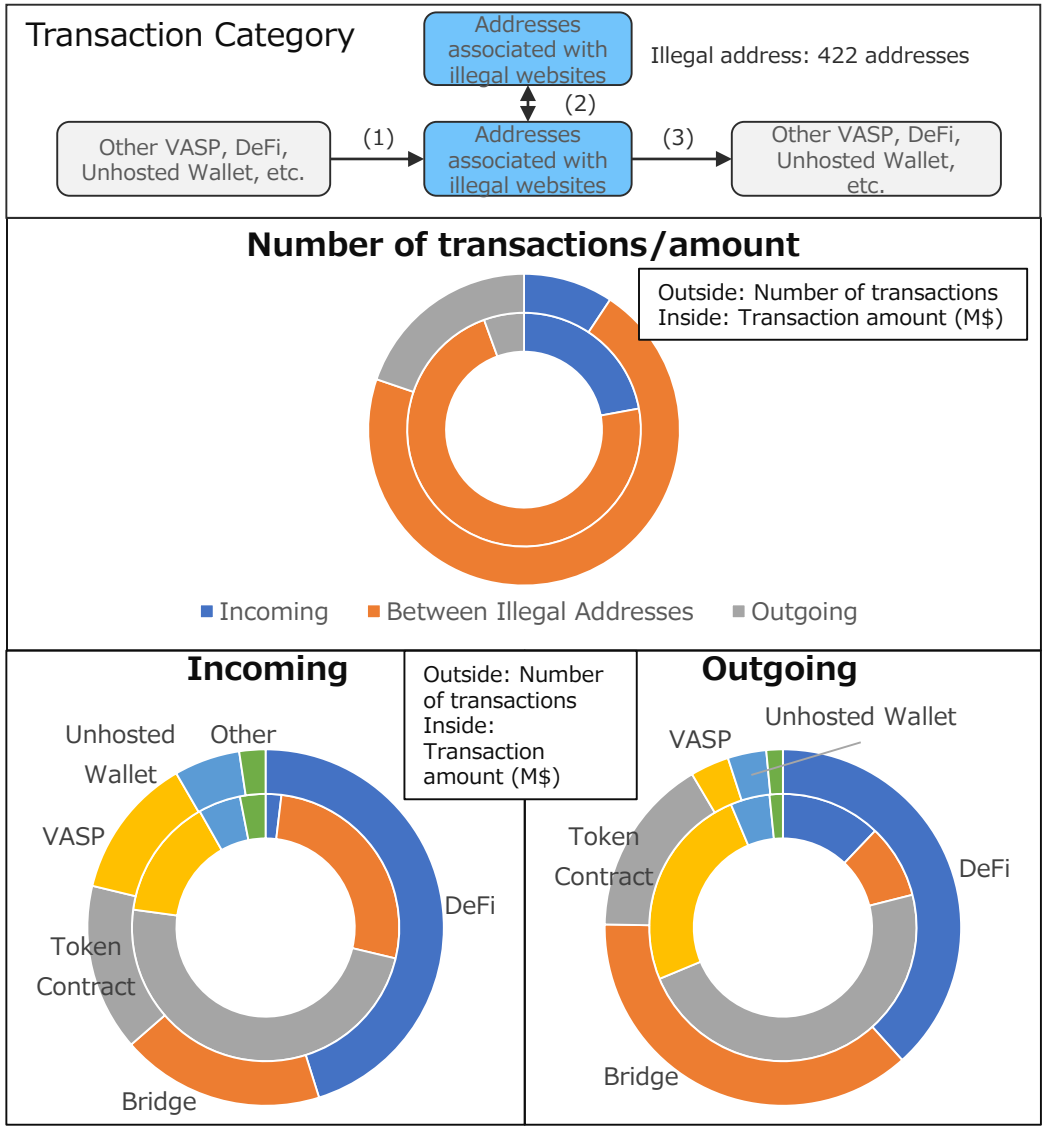



Table 4-4-6-3 Fraud, etc. transactions / amount data by category

| Category | (1) Incoming | | | (2) Between Illegal Addresses | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|---|---|---|
| | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ |
| DeFi | 5,496 | 45.1% | 23 | | | | 9,902 | 38.3% | 37 |
| Bridge | 2,246 | 18.5% | 323 | | | | 9,544 | 36.9% | 27 |
| Token Contract | 1,846 | 15.2% | 584 | | | | 4,187 | 16.2% | 144 |
| VASP | 1,568 | 12.9% | 177 | | | | 910 | 3.5% | 75 |
| Unhosted Wallet | 728 | 6.0% | 62 | | | | 903 | 3.5% | 14 |
| Other | 289 | 2.4% | 37 | | | | 386 | 1.5% | 5 |
| Total | 12,173 | 100.0 | 1,206 | 92,730 | 100.0 | 3,945 | 25,832 | 100.0 | 303 |

| Identification of address holder | (1) Incoming | | | (3) Outgoing | | |
|---|---|---|---|---|---|---|
| | Transactions | Transaction ratio | Amount M$ | Transactions | Transaction ratio | Amount M$ |
| Identified address holders | 25,832 | 14.3% | 303 | 12,173 | 13.7% | 1,206 |
| Unknown address holders | 154,762 | 85.7% | 3,002 | 76,399 | 86.3% | 2,267 |
| Total | 180,594 | 100.0% | 3,305 | 88,572 | 100.0% | 3,472 |

[Discussion]

- The largest number and amount of transactions were “(2) Between Illegal Addresses”
  → Possible that large number of internal transactions are executed by dummies to prevent transactions from being identified. (e.g., mixing services)
- The largest number of transactions by category was DeFi for both “(1) Incoming” and “(3) Outgoing”. The largest transaction amount was Token Contract.
  → DeFi is considered to be token exchange by decentralized exchanges such as Uniswap for both “(1) Incoming” and “(3) Outgoing”, and token contract is considered to be by token transfer (mainly WETH, etc.).

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-6. AML/CFT Related

(4) Number and amount of transactions for addresses remittance from online gambling services

Figure 4-4-6-4 Gambling services number of transactions / amount by category

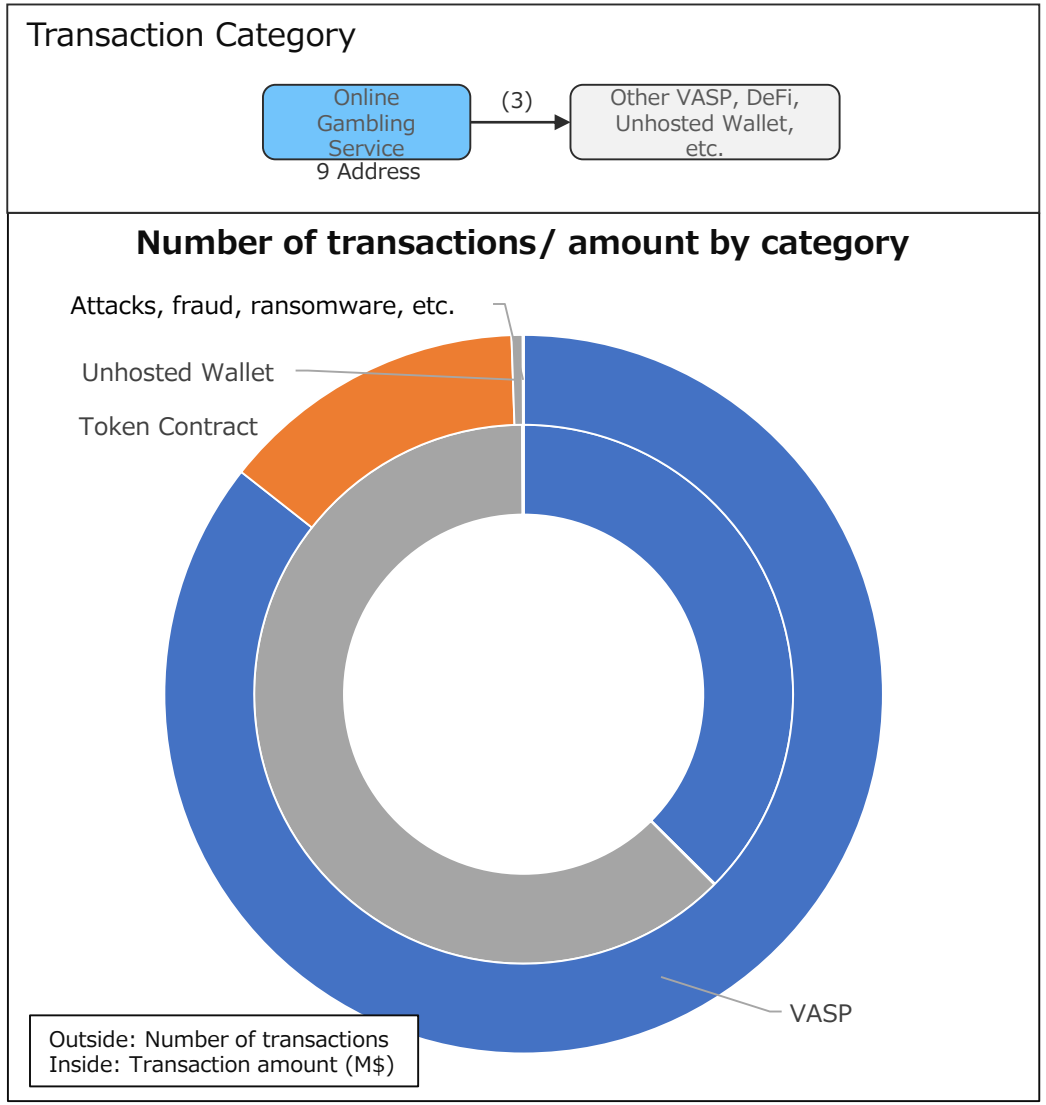



Table 4-4-6-4 Gambling services transactions / amount data by category

| Category | (3) Outgoing | | |
|---|---|---|---|
| | Number of transactions | Transactions Ratio | Amount M$ |
| VASP | 24,495 | 85.6% | 8 |
| Token Contract | 3,961 | 13.8% | 0 |
| Unhosted Wallet | 143 | 0.5% | 13 |
| Attacks, fraud, ransomware, etc. | 12 | 0.0 | 0 |
| Total | 28,611 | 100.0 | 21 |

| Identification of address holder | (3) Outgoing | | |
|---|---|---|---|
| | Number of transactions | Transactions Ratio | Amount M$ |
| Identified address holders | 28,611 | 7.4% (1) | 21 |
| Unknown address holders | 357,354 | 92.6% (%) | 874 |
| Total | 385,965 | 100.0 | 895 |

[Discussion]

- By category, VASPs are the largest number of transactions.
  → Wallets of major VASPs are most likely to be used as a destination for money transfers for online gambling services
- The next large number of transaction is token contract.
  → This is considered to be for the transfer of stablecoins (USDC, DAI, etc.)

(5) Number and amount of transactions for addresses transferred from the mixing service

Figure 4-4-6-5 Mixing services number of transactions / amount by category

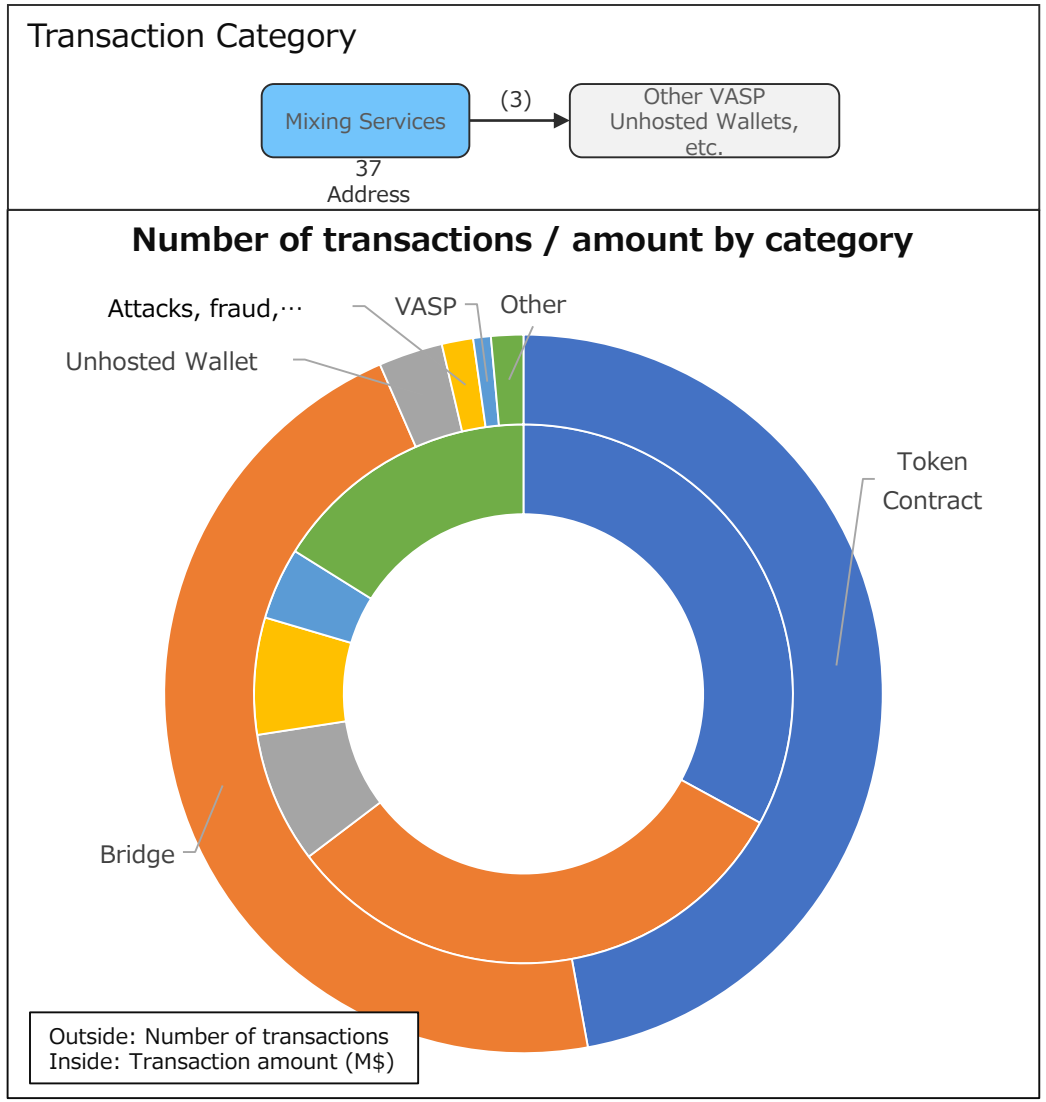



Table 4-4-6-5 Mixing services transactions / amount data by category

| Category | (3) Outgoing | | |
|---|---|---|---|
| | Number of transactions | Transactions Ratio | Amount M$ |
| Token Contract | 9,341 | 47.1% | 22 |
| Bridge | 9,183 | 46.3% | 22 |
| Unhosted Wallet | 572 | 2.9% | 5 |
| Attacks, fraud, ransomware, etc. | 280 | 1.4% | 5 |
| VASP | 157 | 0.8% | 3 |
| Other | 287 | 1.4% | 11 |
| Total | 19,820 | 100.0 | 68 |

| Identification of address holder | (3) Outgoing | | |
|---|---|---|---|
| | Number of transactions | Transactions Ratio | Amount M$ |
| Identified address holders | 19,820 | 11.7% | 68 |
| Unknown address holders | 148,879 | 88.3% | 2,491 |
| Total | 168,699 | 100.0% | 2,560 |

[Discussion]

- By category, token contracts are the largest number of transactions.
  → Likely used for money transfers (mainly WETH, etc.) to access mixing services.
- The next large number of transactions is Bridge (transferring funds to other chains).
  → This is considered to transfer of mixing funds on Ethereum blockchain to other blockchains.

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (1/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Transactions | Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record keeping or reporting thresholds, similar to structuring cash transactions | User (account) address | Etherscan<br>In-house database | Obtain addresses where small transactions of less than 0.1 ETH (approx. 25,000 yen) were sent | 65,482 addresses<br>[Breakdown]<br>VASP 42,889,<br>Unhosted Wallet 11,362, etc. | 27,013,172 addresses | VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |
| | | Number of transactions and value of transactions at the above addresses | Etherscan<br>In-house database | Obtain the number of transactions and amount of money for the above address | Number of transactions:<br>69,669,928<br>Amount: 4.61 billion USD | Number of transactions:<br>167,267,783<br>Amount: 9.14 billion USD | |
| | Making multiple high value transactions in short succession, such as within a 24 hour period | User (account) address | Etherscan<br>In-house database | Get addresses where the same sender has sent transactions of 10 ETH (approx. 18,000 USD) or more in the last 24 hours | 3,351 addresses<br>[Breakdown]<br>VASP 1,436,<br>Unhosted Wallet 846, etc. | 59,127 addresses | |
| | | Number of transactions and value of transactions at the above addresses | Etherscan<br>In-house database | Obtain the number of transactions and amount of money for the above address | Number of transactions:2,631,151<br>Amount: 810.9 billion USD | Number of transactions:3,874,440<br>Amount: 1,202.7 billion USD | |
| | | Frequency of transactions at the above addresses | Etherscan<br>In-house database | Obtain the ratio of the number of transactions by time for the above transactions | Within 1 hour: 88.4%,<br>1-12 hours: 10.1%,<br>13-24 hours: 1.5% | - | |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (2/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Transactions | Making multiple high value transactions to a newly created or to a previously inactive account | User (account) address | Etherscan<br>In-house database | Get addresses that have sent 10 ETH or more transactions within 24 hours of the address's first deposit | 703 Addresses<br>[Breakdown]<br>Unhosted Wallet 335, VASP 151, etc. | 213,668 addresses | VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |
| | | Number of transactions and value of transactions at the above addresses | Etherscan<br>In-house database | Obtain the number of transactions and amount of money for the above address | Number of transactions: 2,164<br>Amount: 885 million USD | Number of transactions: 259,264<br>Amount: 74.56 billion USD | |
| | | Frequency of transactions within a certain period of time for the above addresses | Etherscan<br>In-house database | Obtain the ratio of the number of transactions by time for the above transactions | Within 1 hour: 36.5%,<br>1-12 hours: 57.5%,<br>13-24 hours: 6.0% | - | |
| | | Number of transactions at the above address | Etherscan<br>In-house database | Obtain the number of transactions by time for the above transactions | Within 1 hour: 813,<br>1-12 hours: 1,280,<br>13-24 hours: 132 | | |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (3/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Transactions | Transferring VAs immediately to multiple VASPs | User (account) identification | Etherscan<br>In-house database | Obtain wallets to send to multiple VASPs | 997 addresses<br>[Breakdown]<br>Unhosted Wallet 731,<br>VASP 200, etc. | 1,086 addresses | VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |
| | | Identification of VASPs, etc. | Etherscan<br>In-house database | Identify the VASPs sent by the above wallets | 9,268 addresses | - | |
| | Accepting funds suspected as stolen or fraudulent depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds | Addresses that are being misused | Etherscan<br>In-house database | Obtain addresses of known attackers | 422 addresses | - | - |
| | | Address of the counterparty to the above address | Etherscan<br>In-house database | Obtain a wallet to send to known attackers | 4,191 addresses<br>[Breakdown]<br>VASP 1,567,<br>Unhosted Wallet 1,285,<br>etc. | 163,109 addresses | VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (4/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Transaction Patterns | A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform | New User Accounts | Etherscan<br>In-house database | Get a new user for VASP | 137 addresses | 57,415 addresses | -<br>VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |
| | | All balance transactions made by the above accounts | Etherscan<br>In-house database | Calculate the user's balance and obtain the transaction that empties the balance | 175 transactions | 75,993 transactions | |
| | Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account | User (account) address | Etherscan<br>In-house database | Obtain the same address from multiple addresses that have been remitted to repeatedly | 106 addresses<br>[Breakdown]<br>Fraud/Attackers 28,<br>VASP 23m<br>Unhosted Wallet 12, etc. | 25,543 addresses | |
| | | Number of transactions and value of transactions at the above addresses | Etherscan<br>In-house database | Obtain the number of transactions and amount of money for the above address | Number of transactions: 21,338<br>Amount: 50.87 million USD | Number of transactions: 1,688,075<br>Amount: 1.46 billion USD | |
| | | Frequency of transactions at the above addresses | Etherscan<br>In-house database | Obtain the ratio of the number of transactions by time for the above transactions | Within 1 hour: 44.3%,<br>Within 24 hours: 54.7%,<br>1 day - 30 days: 1.0% | - | |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (5/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Anonymity | VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms | Address of VASP, which operates mixing and tumbling services and P2P platforms | Etherscan<br>In-house database | Obtain VASP address with mixing service | 116 addresses | - | VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |
| | | Addresses such as wallet (user account) where transactions were made with mixing services, etc. | Etherscan<br>In-house database | Obtain addresses of hosted/unhosted wallets, etc., where mixing services, etc., have been transacted | 33,236 addresses<br>[Breakdown]<br>VASP 22,257,<br>Unhosted Wallet 6,304,<br>etc. | 9,035,176 addresses | |
| | Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces | Addresses with transactions using mixing and tumbling services. | Etherscan<br>In-house database | Obtain the address of the mixing service | 37 Addresses<br>All Tornado Cash<br>*Related tools include Railgun<br>*OFAC sanctioned list of 90 addresses (26 of which overlap) | - | |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (6/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Anonymity | Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports | Data identifying known and suspected sources of information | Etherscan, DappRadar, IC3, CISA, OFAC In-house database | Obtain rogue wallet addresses linked to the darknet from DappRadar, IC3, CISA, and OFAC | 12 addresses Identify the URL of the Darknet Web and the address associated with it. | - | |
| | | Addresses that have done business with the above questionable sources | Etherscan, DappRadar, IC3, CISA, OFAC In-house database | Obtain the above fraudulent address and the address where the transaction took place | Sent: 38 addresses/50 items Received: 4 addresses/5 items | Sent: 38 addresses/50 items Received: 143 addresses/ 193 items | |
| | Receiving funds from or sending funds to VASPs whose CDD or know-your-customer (KYC) processes are demonstrably weak or non-existent. | Identification of VASPs that appear to have no CDD/KYC process at the time of joining the VASP | Etherscan In-house database | Obtain addresses of VASPs that do not appear to have CDD/KYC processes when joining VASPs | 788 Addresses *Get the address of a VASP that is not decentralized and not registered in the location | - | If a VASP itself identifies an unregistered VASP in the process of conducting due diligence on a counterparty VASP, is it possible to provide information to the authorities, etc.? |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (7/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators about Senders or Recipients | A customer's VA address appears on public forums associated with illegal activity | Address of unauthorized transactions | Etherscan, Reddit Bulletin Board, Darknet forums & marketplaces In-house database | Obtain unauthorized wallet addresses linked to the darknet from DappRadar, Reddit message boards, and darknet forums | 12 addresses | - | Is it possible for VASPs themselves to provide information to the authorities by reporting suspicious transactions, etc., if they discover fraudulent transactions by their customers? |
| | A customer is known via publicly available information to law enforcement due to previous criminal association | Address of unauthorized transactions | Etherscan, IC3, CISA, OFAC In-house database | Collect sanctioned addresses published in IC3, CISA, and OFAC | Sent: 50 addresses/ 61 transactions Received: 61 addresses/74 transactions | Sent: 629 addresses/ 2,224 transactions Received: 311 addresses/ 580 transactions | |
| Red Flag Indicators in the Source of Funds or Wealth | Transacting with VA addresses that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites | Cryptographic asset addresses associated with illegal websites | CISO OFAC ,. Threat Intelligence (Darknet), CISA, IC3 , CSAM Data (Hades) In-house database | Identify addresses associated with fraud and extortion, ransomware schemes, sanctioned addresses, darknet marketplaces, or other illegal websites | Sent: 2,407 addresses/ 117,650 transactions Received: 142 addresses/ 14,357 transactions | Sent: 56,235 addresses/ 264,817 transactions Received: 172 addresses/ 91,344 transactions | |
| | VA transactions originating from or destined to online gambling services | Addresses of users of online gambling services | Etherscan Word Cloud, ETHplorer.io In-house database | Identify the address of the online gambling service and obtain the address of the transaction using that address | Sent: Gambling 7 addresses, User 257 addresses/ 28,742 transactions Received: Gambling 2 addresses, User 2 addresses, 3 transactions | Sent: Gambling 13 addresses, User 102,392 addresses/ 386,225 transactions Received: Gambling 11 Addresses, User 113,524 addresses/ 627,912 transactions | |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (8/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators in the Source of Funds or Wealth | A customer's funds which are sourced directly from third-party mixing services or wallet tumblers | Addresses with transactions using mixing and tumbling services. | Etherscan<br>In-house database | obtain the remitted address from the mixing service | Mixing 37 addresses,<br>Recipients 769 addresses/<br>19,820 transactions | Recipients 53,268 addresses/<br>168,699 transactions | Is it possible for VASPs themselves to provide information to the authorities by reporting suspicious transactions, etc., if they discover fraudulent transactions by their customers? |
| | Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc. | Address of unauthorized transactions | Etherscan<br>In-house database | obtain addresses transferred from known fraudulent/fraudulent addresses | Fraud/Illicit 147 addresses,<br>Recipients 59 addresses/<br>1,121 transactions | Fraud/Illicit 1,142 addresses,<br>Recipients 1,186 addresses/<br>4,742 transactions | |
| Red Flag Indicators Related to Geographical Risks | Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located | Addresses of exchanges not registered in the jurisdiction in which they are located | Etherscan<br>In-house database | Obtain the address of the VASP for transactions transferred to the user from a VASP that is not registered in the jurisdiction in which it is located | 139 addresses | - | VASP stores CDD/EDD information in association with the user's address.<br>Is it possible to narrow down and report suspicious transactions with a higher degree of certainty by combining with the left column? |
| | | User addresses transferred from exchanges that are not registered in your jurisdiction | Etherscan<br>In-house database | Obtain the user's address for transactions transferred to the user from a VASP that is not registered in the jurisdiction in which it is located | 8,275 addresses<br>[Breakdown]<br>VASP 8,266 addresses<br>(including hosted wallets) 8,266,<br>Other 9, etc. | - | |

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

(6) AML/CFT related

Table 4-4-6-6 AML/CFT data survey results (9/9)

| Category | Surveyed Items | Surveyed Data | Research Results | | | | Data held and investigative potential of supervised entities |
|---|---|---|---|---|---|---|---|
| | | | Data Source | Data Obtaining Method | Data Obtaining Results *1 | Data Obtaining Results *2 | |
| Red Flag Indicators Related to Geographical Risks | Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls. | Identification of jurisdictions requiring attention | Etherscan, OFAC, In-house database | Obtain countries on the OFAC Sanctioned Countries List and U.S. Military Export Prohibited Countries List | 49 countries/regions*<br>(1) List of OFAC sanctioned 25 countries/regions,<br>(2) List of U.S. military export prohibited 24 countries/regions<br>*(1) and (2) include duplicates. | - | • same as above<br>• VASPs themselves should be utilized after confirming that there are no differences between the high-risk countries, etc. defined by the blockchain analytics company and the settings on the tool side. |

*[Jurisdictions requiring attention] 49 countries/regions
(1) List of 25 OFAC sanctioned countries/regions https://ofac.treasury.gov/sanctions-programs-and-country-information
Afghanistan, Balkans, Belarus, Myanmar, Central Africa, China, Cuba, North Korea, Congo, Ethiopia, Hong Kong, Iran, Iraq, Lebanon, Libya, Mali, Nicaragua, Somalia, South Sudan, Sudan, Syria, Russia, Venezuela, Yemen, Zimbabwe
(2) List of 24 U.S. military export prohibited countries/regions https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-126/section-126.1
Belarus, Myanmar, China, Cuba, Iran, North Korea, Syria, Venezuela, Afghanistan, Cambodia, Central Africa, Cyprus, Congo, Ethiopia, Eritrea, Haiti, Iraq, Lebanon, Libya, Russia, Somalia, South Sudan, Sudan, Zimbabwe

*1: Data Obtaining Results: Survey results for addresses for which the blockchain analytics company identified category names and account names
*2: Data Obtaining Results: All data obtained in this survey (including addresses for which category names, etc., were not identified)

# 4-4. Results of AML/CFT-Related Data Analysis
## 4-4-7. Main Findings

Table 4-4-7 Main Findings

| Main Findings | Contents |
|---|---|
| Certain usefulness of research of experts compared to blockchain analytic tools | • Regarding the possibility of acquiring the data pointed out in the FATF report, among the AML/CFT-related data examined in this study, many of the data were difficult to obtain using analytical tools, but many of the data could be obtained using research by experts. In addition to analytical tools, experts can also be used to understand AML/CFT-related data.<br>• However, since this study also confirmed the existence of a certain number of data that are difficult to obtain, it will be necessary in the future to clarify the possibility of obtaining such data, including the provision of information by supervisors. |
| Difficulty in high-risk determination | • Although many VASP-related transactions are classified as "high-risk" under the definition of high-risk addresses and transactions (VASP-related addresses with an extremely large number of transactions are labeled as "high-risk"), it is highly likely that many transactions related to such addresses are normal transactions, and it is difficult to draw a general conclusion from the results of this survey.<br>• Although many of the addresses with unidentified accounts may be considered to be unhosted wallets, the nature of the risk is unknown, and it is extremely difficult to accurately understand the actual situation (e.g., volume of transactions) and assess the risk of P2P and other types of transactions. |
| Close interconnection between VASP, Unhosted Wallet (including P2P), and DeFi | • In addition to transactions between VASPs, close business relationships existed between VASPs, unhosted wallets (including P2P), and DeFi, and a significant number of high-risk transactions were identified (although difficult to define).<br>• In order to reduce ML/TF/PF risk for P2P and highly decentralized DeFi, which are not regulated in many jurisdictions, and taking into account the difficulties of data analysis for unhosted wallets and P2P mentioned above, it is possible that stronger controls on VASPs, which are relatively easier to deal with in terms of regulatory measures (such as EDDs for transactions between VASPs and unhosted wallets, etc.) may be effective. |
| Need for efforts to improve the reliability of data and data analysis | • The results of this research confirmed that only about 10% of the Ethereum blockchain data had been identified by the blockchain analytics companies as category or account names, which means that the company was not necessarily able to analyze data from the entire decentralized financial system.<br>• The category and account names identified, as well as the determination of high-risk transactions, all rely on information from blockchain analytics companies, and since the identification of account names, etc. and the calculation of risk scores are done independently by blockchain analytics companies, the content may differ from one analytics company to another.<br>• Therefore, when conducting a fact-finding survey, it is considered necessary to improve the reliability of the data by not relying on data from a single company, for example, by comparing survey results from multiple analysis companies. |

# Chapter 5: Conclusion

# Chapter 5: Conclusion

(1) Insights gained from conducting data analysis

- A certain amount of training is required for financial authorities to properly use analytical tools and researchers. It is also necessary to understand the limitations of the current tools.
  (It is not a silver bullet that will significantly improve monitoring capabilities.)
  - Sanitization of data obtained from tools and researchers (e.g., removal of outliers) and understanding of context (e.g., that token contract-related transactions are not actual token transfers, but rather smart contract behavior associated with transfers between addresses (EOAs) such as stablecoins) are required.
  - Tool companies and solutions vary (some are specialized for investigative authorities, others are mainly used by businesses rather than authorities), and it is necessary to select the right tool for the right application, understand the overall picture of tools, and gather information on the latest technology trends.
- On the other hand, there is a possibility that the tools may provide useful insights into the interconnections in the crypto asset market (e.g., connections between VASPs, unhosted wallets, and DeFi) and the actual state of illicit transactions, including those not subject to regulatory oversight (DeFi, P2P, etc.), and the identification rate and accuracy of the tools will improve in the future. Should the use of tools and researchers be explored, taking into account the possibility that the identification rate and accuracy of tools will improve in the future?

(2) Initial Financial Regulatory Implications

- Given the close relationship between regulated entities (VASPs) and others (unhosted wallets, P2P, (fully decentralized) DeFi), the possibility that strengthening controls over VASPs could indirectly reduce the risk of P2P and other unregulated activities.
- There are many smart contract related transactions on Ethereum, such as DeFi, ERC-20 related token contracts (e.g. stablecoin), and bridges. Hacking, etc., has been frequent, and is improving security a major issue?
- Although it is possible to identify addresses that appear to be involved in crimes, it is not easy to identify the actual owners, etc. (The analysis tools used in this research were not intended for criminal investigations, but specialized analysis tools may yield different results).

# Appendix

# Appendix 1. Data Analysis Methods Utilized in the Research Literature

(1) Data analysis methods of the research literature

- We surveyed the main research literature analyzing on-chain/off-chain data to understand the actual status of blockchain, and investigated the data analysis methods used.
- The investigation identified multiple analytical methods utilizing address clustering and graph theory/machine learning for the purpose of identifying multiple account administrators and suspicious transactions for blockchain addresses.
- However, the results of the research are limited to understanding overall trends and identifying some target addresses, and analysis from publicly available on-chain/off-chain data is considered to be limited in understanding the actual status of the blockchain.

Table A-1-1 Methods of data analysis of research literature

| Data distinction | Data Analysis Methodology | Overview of Analysis Methodology | Results of a research |
|---|---|---|---|
| On-chain data analysis | Clustering | • Grouping blockchain addresses and other data analysis methods into broad groups of desired data | • The following three studies on clustering of blockchain addresses were identified<br>➢ Addresses appearing in the input of a transaction<br>➢ Classification of addresses by transaction patterns such as address reuse and airdrop (token distribution)<br>➢ Bloom filter (probabilistic data structure) to characterize addresses, etc. |
| | Graph Theory | • Applying mathematical theory, which consists of a set of nodes (vertices) and edges (lines connecting nodes), the characteristics of nodes and edges are analyzed based on relationships such as their concentration, with nodes as blockchain addresses and edges as transactions. | • Confirmed that graph theory has been studied in clustering blockchain addresses and analyzing transaction trends |
| | Machine Learning | • Build models based on sample data and make predictions (judgments) without being explicitly programmed<br>• Multiple algorithms exist for different learning methods (supervised learning, unsupervised learning, reinforcement learning, etc.) | • Of the machine learning, the following three analysis methods were identified as being studied, including detection of illegal addresses<br>➢ Random Forest<br>➢ Support Vector Machine<br>➢ XGBoost |
| | Other | • Investigate methods of analyzing on-chain data other than those listed above | • Identified 1 case of analysis of smart contract code and transaction logs (Analyzed behavior suspected to be a ponzi scheme and investigated with detection tools) |
| Off-chain data analysis | Publicly available data screening | • Using publicly available off-chain data to select valid data for blockchain analysis | • The following three data analysis cases were identified<br>➢ Twitter's 'Whale Alert' Tied to Bitcoin Price Rise<br>➢ Identifying criminal activity-related addresses from public blockchain posting sites<br>➢ Search academic databases and journals to investigate market manipulation techniques, etc. |

# Appendix 1. Data Analysis Methods Utilized in the Research Literature

(2) Research literature survey results

Table A-1-2 Results of research literature survey (1/5)

| No. | Source | Document-name | Summary | On-chain data analysis | | | | Off-chain data analysis |
|---|---|---|---|---|---|---|---|---|
| | | | | Clustering | Graph Theory | Machine Learning | Other | |
| 1-1 | The Journal of Finance Volume 75, Issue 4 | Is Bitcoin Really Untethered? | • Analysis of blockchain data from October 2014 to March 2018 on Bitcoin's relationship with Tether (USDT: a stablecoin pegged to the US dollar) to price increases.<br>• Reported speculation of market manipulation of the Bitcoin price through the issuance of Tether | Grouping addresses that appear in the transaction input | | | | |
| 1-2 | Finance Research Letters Volume 49 | The Intraday Bitcoin Response to Tether Minting and Burning Events: Asymmetry, Investor Sentiment, and "Whale Alerts" on Twitter | • Analyzed blockchain data from October 2014 to January 2021, when Tether was issued, to investigate Bitcoin's response to Tether's issuance.<br>• Investigators reported that Tether's issuance event was a "Whale Alert" notifying Twitter of high-value transactions in near real-time, and positive investor sentiment drove Bitcoin prices higher. | | | | | Analyzing Whale Alert's Twitter Announcement and Bitcoin's Price Rise |
| 2 | Financial Cryptography and Data Security 2020 | Address Clustering Heuristics for Ethereum | • Clustering Ethereum addresses based on transaction patterns such as address reuse and airdrops to analyze entities that are likely to be managing multiple accounts<br>• Approximately 18% of Ethereum addresses can be clustered, identifying more than 340,000 entities managing multiple addresses | Grouping of addresses based on transaction patterns such as address reuse, airdrop, etc. | | | | |

# Appendix 1. Data Analysis Methods Utilized in the Research Literature

(2) Research literature survey results

Table A-1-2 Results of research literature survey (2/5)

| No. | Source | Document-name | Summary | On-chain data analysis | | | | Off-chain data analysis |
|---|---|---|---|---|---|---|---|---|
| | | | | Clustering | Graph Theory | Machine Learning | Other | |
| 3 | 2021 IEEE International Conference on Decentralized Applications and Infrastructures | Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users | • Research on how to identify users by association of Ethereum addresses using machine learning with graph theory<br>• User profiling explains superiority of node embedding method | Research methods for identifying users by clustering addresses | Utilize graph theory (node embedding technique) for data analysis | Leveraging machine learning for data analysis | | |
| 4 | 30th USENIX Security Symposium | Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain | • Researching methods to efficiently measure the behavior of Ethereum front-running attacks (attacks in which miners intentionally swap transactions during block generation to gain profit).<br>• Identified approximately 200,000 attack transactions, 1.5,000 attacker accounts, bots, profit amounts, etc. | Bloom filter (probabilistic data structure) to group attacker addresses | | | | |
| 5 | IEEE INFOCOM 2018 - IEEE Conference on Computer Communications | Understanding Ethereum via Graph Analysis | • Graph-theoretic analysis of Ethereum transaction data for an approach to security issues.<br>➢ Attack Forensics: Detection of malicious smart contract attacker accounts<br>➢ Anomaly detection: detection of accounts that create a large number of smart contracts that are not invoked<br>➢ De-anonymization: extract important keywords from information such as comments about nodes | | Money Flow/ Smart Contract Creation/Smart Contract Calling Analyzed by Graph Theory | | | |

# Appendix 1. Data Analysis Methods Utilized in the Research Literature

(2) Research literature survey results

Table A-1-2 Results of research literature survey (3/5)

| No. | Source | Document-name | Summary | On-chain data analysis | | | | Off-chain data analysis |
|---|---|---|---|---|---|---|---|---|
| | | | | Clustering | Graph Theory | Machine Learning | Other | |
| 6 | FC 2019: Financial Cryptography and Data Security | Measuring Ethereum-based ERC20 Token Networks | • Graph theory analysis of the relationship between Ethereum's top 1,000 token transfers and token owners.<br>• While the majority of token transfers are concentrated on exchanges and other venues, we found that many token holders do not move their tokens at all | | Graph theory analysis of token transfers and token holders | | | |
| 7 | WWW '20: Proceedings of The Web Conference 2020 | Measurements, Analyses, and Insights on the Entire Ethereum Blockchain Network | • Analyze the interaction of Ethereum users, transactions, smart contracts, token transfers, etc. using graph theory to study similarities and differences with SNS and the Web.<br>• Explain that the distribution of transactions is different from that of social networking sites, etc. | | Graph theory analysis of relevance of transactions, token transfers, etc. | 【Machine Learning Algorithm】<br>• Random Forest:<br>Algorithm in which multiple decision trees trained in parallel are asked to make predictions, and the final output is determined by majority vote or average.<br>• Support Vector Machines:<br>Algorithms for classification and regression by determining boundaries, etc. that divide two classes of data groups.<br>• XGBoost:<br>An algorithm that combines ensemble learning (a method of outputting comprehensive results using multiple methods that do not have high performance) and decision trees (a method of solving problems by conditional branching), called gradient boosting. | | |
| 8 | Financial Cryptography and Data Security 2023 Accepted papers | Understanding Polkadot Through Graph Analysis: Transaction Model, Network Properties, and Insights | • Model user transactions in the Polkadot blockchain and analyze them in the Transaction Action Graph<br>• Detecting the concentration of power in Binance and the reality that the majority of native tokens are occupied by 2% of users. | | Graph Theory Analysis of User Transaction Concentration | | | |
| 9 | Web Information Systems Engineering - WISE 2019 | Detecting Fraudulent Accounts on Blockchain:. A Supervised Approach | • Comparing three machine learning analysis methods for the purpose of detecting fraudulent accounts of malicious actors<br>• Random forests yielded the best results in reproducibility and false positive rate | | | Comparing three methods: random forests, support vector machines, and XGBoost | | |

# Appendix 1. Data Analysis Methods Utilized in the Research Literature

(2) Research literature survey results

Table A-1-2 Results of research literature survey (4/5)

| No. | Source | Document-name | Summary | On-chain data analysis | | | | Off-chain data analysis |
|---|---|---|---|---|---|---|---|---|
| | | | | Clustering | Graph Theory | Machine Learning | Other | |
| 10 | Expert Systems with Applications Volume 150 | Detection of illicit accounts over the Ethereum Blockchain | • Detect illegal activity in transaction history using XGBoost based on approximately 2,000 addresses flagged as illegal by the Ethereum community (Etherscam DB) and normal addresses<br>• Achieved an average accuracy of 96% with 10 cross-validations | | | Use XGBoost for data analysis | | EtherscamDB information is tied to an Ethereum account |
| 11 | Future Generation Computer Systems Volume 102 | Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact | • Investigate ponzi schemes (investment fraud) on Ethereum and analyze behavior and impact<br>• Analyzed smart contract code and transaction logs for suspected ponge scheme behavior using validation tools and identified 184 ponge schemes | | | | Analyze smart contract code and transaction logs to identify ponge schemes | |
| 12 | ICIS 2021 - International Conference on Information Systems | Cryptocurrency Market Manipulation: A Systematic Literature Review | • Keyword search of 7 academic databases and 3 leading journal journals for market manipulation of crypto assets<br>• Analysis identifies 7 major methods of market manipulation (Pump&Dump, money laundering, order books, stablecoin, front running, insider trading, DDOS attacks) | | | | | Academic databases, keyword searches of leading journals to analyze trends |

# Appendix 1. Data Analysis Methods Utilized in the Research Literature

(2) Research literature survey results

Table A-1-2 Results of research literature survey (5/5)

| No. | Source | Document-name | Summary | On-chain data analysis | | | | Off-chain data analysis |
|---|---|---|---|---|---|---|---|---|
| | | | | Clustering | Graph Theory | Machine Learning | Other | |
| 13 | Financial Cryptography and Data Security 2023 Accepted papers | Short paper: DeFi Deception-Uncovering the prevalence of rug pulls in cryptocurrency projects | • Analyzed time to fraud execution and methods related to DeFi's take-away fraud (rug pull) and investigated fraud trends<br>• Fraud has been declining since late 2022 due to IDO (funded by DEX token issuance), NFT, and other new services since then, which have reduced take-away fraud. | | | | | Bitcointalk (discussion forum), analysis of market site information |