Analysis for the Healthy Development of Stablecoins
Research Paper

March 2025

Deloitte Tohmatsu Consulting

Acknowledgments and Disclaimer

Acknowledgments

- In the preparation of this report, we received valuable advice and comments from Professor Naoyuki Iwashita of Kyoto University, Research Professor Shinichiro Matsuo of Georgetown University, and Professor Tetsutaro Uehara of Ritsumeikan University. We also received insightful suggestions and advice from observers at the Bank of Japan and the Digital Agency, as well as officials from the Financial Services Agency.
- Furthermore, we referenced analysis reports from Chainalysis, Elliptic, and TRM Labs, and included some content based on individual interviews.
- Nevertheless, any errors in this report are the sole responsibility of Deloitte Tohmatsu Consulting LLC, the contractor.

Disclaimer

- The contents of this report do not represent the official views of the Financial Services Agency.
- For content other than past or present facts stated in this report, the outlook is based on information available at the time of writing, and actual trends may vary due to various uncertainties.

Background and Purpose of the Study

As stablecoins increase their presence in the market, illicit use of stablecoins have been reported as a pressing challenge in international discussions. This study aims to understand the current situation for the healthy development of stablecoins in the future.

- Stablecoins are considered to have the advantage of avoiding the price volatility risks associated with traditional cryptocurrencies, enabling fast and low-cost remittances and payments. Their use is rapidly expanding among individuals, companies, and institutional investors*1. The scope of their use is not limited to cryptocurrency transaction settlements but extends to international remittances, B2B cross-border transactions, digital payments, e-commerce, and more*2.

  *1 As of January 2025, the market capitalization exceeds $210 billion, with Tether (USDT) being the third-largest cryptocurrency by market capitalization.

  *2 While not yet mainstream as a payment method, stablecoins are becoming more prevalent in some countries and regions by enhancing convenience through connections with existing payment networks (such as international payment brands).

- On the other hand, there are reports from private analysis firms that the illicit use of some stablecoins is expanding, particularly from the perspective of AML/CFT. The FSB has also pointed out that the expansion of stablecoin use poses risks to financial stability, even if not limited to illicit use. Therefore, this study aims to understand the diverse payment uses of stablecoins, analyze their potential risks, and provide insights to maximize the new opportunities brought by stablecoins.
- In this research, we conducted desk research and expert interviews on the following items, compiled the research report (this document), and plan to present it at international conferences. The main readers are stakeholders of stablecoins, and we aim to provide directions for countermeasures against potential risks for future new issuances and use case developments.
  - Investigation of payment-related use cases and surrounding services of stablecoins. We will investigate the actual use of major stablecoins and identify technologies and services that promote their adoption.
  - Investigation of the usage status and illicit use cases of major stablecoins.
    We will systematically organize the overall picture and situation of illicit activities and investigate situations where it is difficult to prevent them with existing countermeasures. The investigation will be conducted at the technical level, including trends in Layer2, non-custodial wallets, and payment services.
  - Investigation of the business realities of major stablecoin issuers.
    We will investigate the business realities of issuers, such as asset management (processes) and promotion activities (partners and surrounding services), and clarify their risk management systems.

Approach

The research status of the investigation and study contents was reported and discussed at regular meetings, expert advice was reflected in the investigation, and a report was compiled.

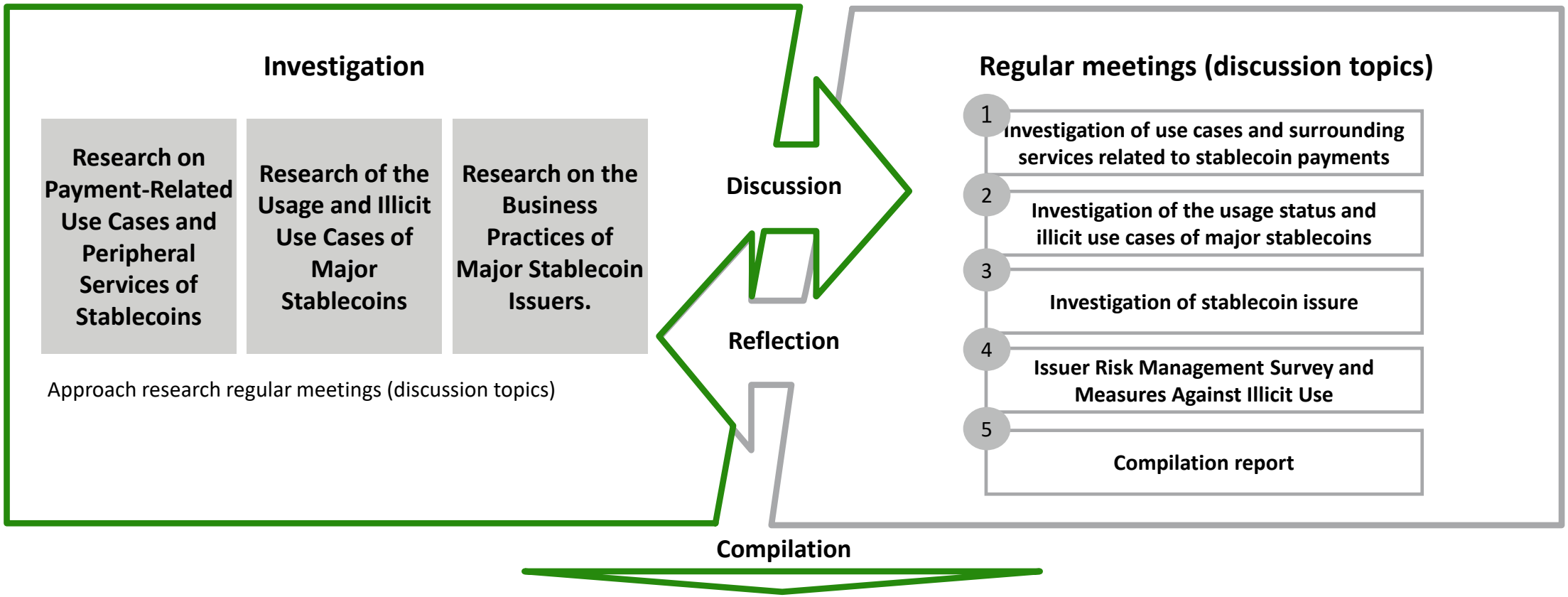


Table of Contents

Glossary

#	Terminology	Definition
1	Smart Contracts	➢ A program deployed on a blockchain that defines rules to be automatically executed when called through transactions. Smart contracts are executed by the blockchain network's nodes. For all results to be valid, the execution results must be recorded on the blockchain.
2	Decentralized Finance (DeFi)	➢ A set of alternative financial markets, products, and systems operated using crypto-assets and "smart contracts" (software) built with technologies that potentially reduce or eliminate the need for centralized or intermediary processes.
3	Decentralized Applications (dapps)	➢ Applications built on a decentralized network that combine smart contracts with front-end user interfaces.
4	Payment Service Providers	➢ Payment service providers are companies or institutions that offer services such as funds transfer, settlement, and clearing in commercial transactions. This includes traditional entities such as credit card companies, electronic money issuers, mobile payment providers, and banks, as well as entities that mediate exchanges when crypto-assets or stablecoins are used as payment methods.
5	Analysis Tool Vendors	➢ Analysis tool vendors specialize in analyzing data recorded on blockchains to provide information that aids in monitoring and tracking crypto-asset transactions. They offer services focused on identifying addresses used for illicit use by analyzing publicly available information outside the blockchain.
6	Wallet Providers	➢ Wallet providers are entities that offer services for storing, sending, receiving, and managing crypto-assets. Wallets are broadly categorized into custodial and non-custodial wallets, and the risks associated with the business vary depending on the type of service provided.
7	FATF	➢ Financial Action Task Force
8	OFAC	➢ The Office of Foreign Assets Control
9	KYC	➢ Know Your Customer
10	AML/CFT	➢ Anti Money Laundering and Combating the Financing of Terrorism

Summary of Research Results

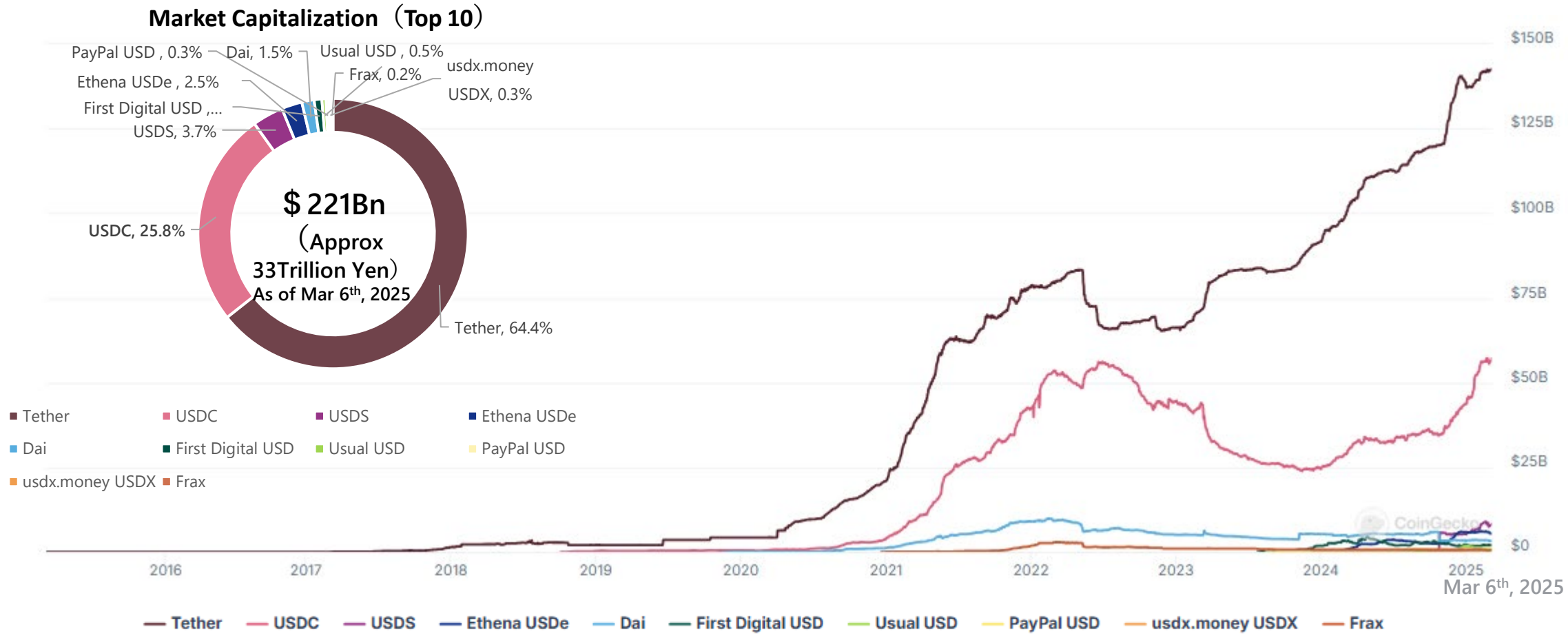
- Stablecoins are primarily used for transactions involving crypto-assets, but their use cases in payments have also been progressing recently. They are mainly utilized in some jurisdictions with low bank account ownership rates or high inflation rates of their national currencies, serving as a store of value alternative to national currencies and as a means of value exchange replacing existing banking networks. In Japan, it is important to continue examining how regulatory authorities, related businesses, and users should respond to these global environmental changes from their respective perspectives.
- Regarding illicit use of stablecoins, which has been a pressing challenge in international discussions, an analysis tool vendor states, "This is a result of recent extensive analysis of transactions involving sanctioned entities, where the percentage of stablecoin usage in this category was relatively high." In other categories, the direct use of crypto-assets remains prevalent. Therefore, it cannot be conclusively said that the expansion of stablecoin use has led to an increase in illicit activities. Rather, it has been confirmed that it is necessary to understand the overall picture, including the instant exchangeability with the underlying crypto-assets, not just the management system of stablecoins themselves.
- To address the illicit use of stablecoins, measures such as the use of blacklist functions by issuers can be considered. However, there are limitations to what issuers can do alone, and cooperation with analysis tool vendors and authorities is required. Additionally, the scope of actors involved in stablecoin transactions has expanded to include not only cash out but also the exchange for goods and services, involving payment service providers, merchants, and other peripheral businesses. Therefore, it is expected that all stakeholders will further fine-tune their measures according to the roles of each actor. On the other hand, compared to traditional finance, there are still many underdeveloped aspects (remaining issues) in terms of regulations and incentives for stakeholders, and efforts toward environmental improvement are still in progress.
- For instance, when an incident is discovered, responses vary, such as immediately freezing assets if there is suspicion (and unfreezing them if the suspicion is cleared later) or consulting authorities before freezing assets (based on multiple analysis tool vendor interviews). Considering the instantaneous cash-out nature of stablecoins, there is a need to strengthen real-time countermeasures. It was also confirmed that there is a need to clarify what constitutes universally recognized illicit activities.
- Furthermore, the technologies used for the illicit use of stablecoins have evolved, including methods like mixing to obfuscate theft routes and chain-hopping across multiple chains. In response to these technologies, there are trends in countermeasures such as stablecoin issuers implementing mechanisms to extend the effectiveness of their blacklists to Layer 2 blockchains, analysis tool vendors using machine learning for pattern analysis, and wallet providers offering alert functions for prevention.
- In understanding the actual situation of stablecoin issuers targeting USDT/USDC, it was confirmed that past issues related to asset management and risk management have been appropriately updated. To ensure that stablecoins can create new opportunities healthily, it is important to leverage the knowledge of these early adopters.
- Additionally, as a reference, we have supplemented the report with details about recent incidents that occurred during the research period, including their background, responses, and tracking status (as of March 7). It was confirmed that some measures, such as partial asset freezing, were effective, and there were cases where sharing the issues identified in past incidents among all stakeholders led to successful countermeasures. Moving forward, to promote the healthy development of stablecoins, the remaining issues presented in the report under "Key Actors and Risk Assessment" should be treated as a to-do list. It is considered that stakeholders should continue to cooperate to mature the nascent industry.

1. Research on Payment-Related Use Cases and Peripheral Services of Stablecoins

1.1 Overview of Stablecoins and Major Stablecoins

Market Capitalization of Major Stablecoins

In December 2024, the market capitalization of stablecoins exceeded 200 billion dollars for the first time and continues to show an increasing trend. Among stablecoins, USDT maintains a high market share, followed by USDC and yield-bearing tokens such as USDe, which are also expanding their shares.



【Reference】「Stablecoins by Market Capitalization」（CoinGecko） as of March 2025、「Top USD Stablecoin Coins Market Cap Chart」（CoinGecko） as of March 2025

Reference: Terra collapse & SVB（Silicon Valley Bank）collapse

Past incidents have indicated the importance of backing stablecoins with fiat currencies and enhancing risk management. This suggests that decentralized finance continues to require the expertise of traditional finance.

【Reference】Terra collapse

Summary and Lessons Learned	【Occurrence Period】：May 7th-9th, 2022 ■ The vulnerabilities of algorithmic stablecoins were exposed, significantly impacting the entire market. The following sequence of events led to the collapse of UST's dollar peg. • In response to the interest rate reduction by Anchor Protocol (a high-yield platform for UST), large investors began to sell off substantial amounts of UST. As a result, the price of UST started to fall below one dollar, leading to widespread panic selling. • As the price of UST declined, a substantial amount of UST was exchanged for LUNA to maintain the peg. Consequently, the supply of LUNA increased dramatically, leading to a collapse (a drop of over 99% within a few days). • This initiated a "death spiral," rendering the value of UST irrecoverable and spreading a crisis of confidence.
Target Coin	■ The Stablecoin Terra USD (UST) and Terra's native token, LUNA. • Price Stabilization Mechanism: When the price of UST exceeds one dollar, LUNA is burned to issue UST, increasing the supply to adjust the price. Conversely, when the price falls below one dollar, UST is burned to issue LUNA, decreasing the supply to adjust the price.
Impact	■ The decline in UST, triggered by a DeFi protocol, caused the algorithm to fail, leading to the collapse of the price peg. This, in turn, caused cascading damage to the following stakeholders: • Individual Investors: Holders of coins/tokens lost more than 99% of value. • Cryptocurrency Exchanges: Platforms such as Binance, FTX, and Coinbase were forced to delist LUNA. • DeFi: Projects on the Terra platform, such as Anchor Protocol, collapsed. • Overall Cryptocurrency Market: BTC and Ethereum also experienced a cascading decline.

Source: Based on "Research Report on Technical Risks in Trust Chains of Decentralized Financial Systems“(Qunie), created by our company, confirmed as of March 2025.

【Reference】SVB（Silicon Valley Bank）collapse

Summary and Lessons Learned	【Occurrence Period】：March 11th-13th, 2023 ■ To ensure the stability of stablecoins, it is necessary to incorporate the knowledge and expertise of traditional finance and to enhance the risk management of backing assets. The following events led to the collapse of the dollar peg for stablecoins: • In response to the Federal Reserve's interest rate hike, the value of SVB's assets significantly declined. With the outflow of deposits, liquidity dried up, leading to SVB's collapse on March 10, 2023. • Fears of frozen deposits caused a sharp decline in USDC. Centralized exchanges (CEX) temporarily halted USDC exchanges due to the massive influx of USDC. Trading on decentralized exchanges (DEX) surged, causing USDC to drop to as low as $0.87, and DAI, in tandem, fell to $0.89. • On March 12, the U.S. Treasury, Federal Reserve, and FDIC announced full protection of deposits, leading to a rapid recovery in USDC's value back to $1.
Target Coin	■ The fiat-collateralized stablecoin USDC and the crypto-collateralized stablecoin DAI. • USDC: Of its reserves (approximately $40 billion), $3.3 billion were deposited in SVB. • DAI: A significant portion of its collateral is held in USDC.
Impact	■ USDC, which had deposited reserves in SVB, and DAI, which used USDC as collateral, significantly lost their value following the bank's collapse. This, in turn, caused cascading damage to the following stakeholders: • USDC Holding Investors: The dollar peg was lost, and the value temporarily dropped to $0.87. • DAI Holding Investors: Following the decline in USDC, the value of DAI also temporarily fell to $0.89. • Cryptocurrency Exchanges: Coinbase and Binance halted USDC exchanges from March 10 to 12.

Source: Based on "Potential Points of Failure for Stablecoins" (BGIN), created by our company, confirmed as of March 2025.

List of Major Stablecoins (Market Capitalization as of March 6, 2025)

As of March 6, 2025, USDT and USDC have significantly large market capitalizations.

#	Coin	Year of Issue	Issuer	Type	Market Cap	Backed Assets	Characteristics
1	**USDT**	2014	Tether Limited /British Virgin Islands	Fiat-Collateralized	**Approx.142.6 B $** (≒**21.1 T ¥**)	USD and Cash Equivalents, Commercial Paper, etc.	➢ U.S. Dollars and Cash Equivalents, Commercial Paper, etc
2	**USDC**	2018	Centre Consortium (Circle/Coinbase PJ)/United States	Fiat-Collateralized	**Approx.57.1 B $** (≒**8.5T ¥**)	USD and Cash Equivalents	➢ The Stablecoin with the Second Largest Market Share after USDT ➢ Monthly audit reports of reserves are published.
3	**USDS**	2024	Sky (Ex. MakerDAO) /United States	Crypto-Collateralized	Approx.8.2 B $ (≒1.2T ¥)	Crypto、SC, USD and Cash Equivalents	➢ USDS incentivizes liquidity providers on the network by distributing a portion of the revenue generated from reserves.
4	**USDE**	2024	Ethena Labs /United States	Strategically Collateralized Synthetic Dollar	Approx.5.4 B $ (≒0.8T ¥)	Crypto Assets, Derivatives	➢ A synthetic stablecoin utilizing cryptocurrency derivatives that is not backed by fiat currency. ➢ Autonomously operated by smart contracts.
5	**DAI**	2017	Maker DAO /United States	Crypto-Collateralized	Approx.3.3 B $ (≒0.49T ¥)	Crypto Assets	➢ Issued with cryptocurrency (such as ETH and WBTC) as collateral. ➢ Collateral assets and DAI issuance are managed by smart contracts.
Ref	**PYUSD**	2023	PayPal, Paxos Trust Company /United States	Fiat-Collateralized	Approx.0.8B $ (≒0.12T ¥)	USD and Cash Equivalents	➢ A stablecoin issued by a major U.S. payment service provider, which can also be used within the PayPal ecosystem. ➢ Operated under the regulation of the New York State Department of Financial Services (NYDFS).
Ref	**BUSD**	2019	Binance, Paxos Trust Company	Fiat-Collateralized	Approx.0.3 B $ (≒45B ¥)	USD and Cash Equivalents	➢ In 2022, it had a market capitalization exceedingly approximately 3 trillion yen, but it significantly decreased after the announcement in August 2023 to gradually cease the handling of "BUSD".
Ref	**EURI**	2024	Banking Circle S.A.	Bank deposit	Approx.0.03 B $ (≒4B ¥)	EUR and Cash Equivalents	➢ The first bank-issued stablecoin compliant with the EU cryptocurrency regulation "Markets in Crypto-Assets (MiCA)".

[References]：「Top Stablecoins by Market Cap」（CoinGecko），「Cryptocurrency Prices, Charts And Market Capitalizations」（CoinMarketCap） as of March 2025

Types of Stablecoins

Among the types of stablecoins, fiat-collateralized stablecoins are mainstream, with USDT and USDC being examples. Recently, yield-bearing stablecoins such as strategically collateralized synthetic dollars have also emerged.

	Overview	Examples of Major Stablecoins
Fiat-collateralized	➢ They are backed by fiat currency or highly liquid assets equivalent to the value of the issued stablecoins. ➢ These stablecoins offer high price stability and reliability but are centralized.	➢ USDT（Tether） ➢ USDC（USDC） ➢ FDUSD（First Digital USD） ➢ PYUSD（Paypal USD） ➢ BUSD（Binance-Peg BUSD）
Bank Issued	➢ Stablecoins issued by banks, backed by the value of fiat currency. ➢ They offer high price stability and have reliability similar to fiat currency, but they are centralized.	➢ EURI（Eurite）
Crypto-collateralized	➢ Multiple cryptocurrencies are deposited, and coins are issued in an amount exceeding the collateral (over-collateralization). ➢ While they offer high transparency, there is a risk that the value of the collateral may plummet due to the price volatility of cryptocurrencies.	➢ USDS（USDS） ➢ DAI（Dai）
Algorithmic, Uncollateralized	➢ Coins that maintain their value through algorithms and market operations without being backed by specific assets. ➢ While they do not require collateral and offer high flexibility, they depend on the design of the algorithm, making them less reliable and with a high risk of collapse.	➢ UST（Terra USD）
Strategy-backed synthetic dollars	➢ Coins that incorporate mechanisms to offset price volatility risks by combining cryptocurrencies and derivatives. ➢ While they offer the potential for high yields, they are highly dependent on market liquidity and volatility, making them high-risk.	➢ USDE（Ethena USDe）

Reference: Strategically Collateralized Synthetic Dollar (Ethena USDe)

The representative of strategically collateralized synthetic dollars, USDE, combines the staking of collateral assets like ETH with derivatives to provide users with stable value and yields, which contributes to its widespread adoption.

Basic Information

Stablecoin overview	■ USDe is an emerging synthetic dollar stablecoin developed by Ethena Labs.
Feature	■ By combining physical ETH with ETH derivatives (short positions in futures), Ethena USDe generates returns through (1) staking of ETH and (2) management of derivatives, providing users with stable value and yields. 1 COLLATERAL 1 ×Long Spot sUSDe 2 DERIVATIVE 1×Short Future **Collateral Asset**: ETH / Derivatives (short position of ETH futures)
Process of Issuing	① After meeting the KYC/AML checks, users are whitelisted by the Ethena protocol. ② Users select stETH (staked ETH) as collateral, determine the amount of USDe to receive, and request issuance. ③ Users deposit stETH into the Ethena system, and an equivalent value of USDe is issued. ④ Simultaneously, an equivalent amount of ETH futures short positions is established. ⑤ Users earn revenue by staking USDe.
Situation	■ USDe reached a supply of $3 billion within just four months after its release. This is attributed to the increasing demand for stablecoins in the DeFi market and the attractive high yields offered by USDe.

Mechanism for Providing Yields and Stabilizing Value

1 ETH staking revenue

Staking Revenue

Staking the ETH deposited at the time of USDe issuance (stETH) and receiving staking rewards.

2 Hedging through derivatives and the spread revenue generated from it

Collateral Value Stability

By selling an equivalent amount of ETH futures, the price of ETH at the time of USDe issuance can be stabilized (delta-neutral strategy).
If the price of ETH decreases, the profits from selling ETH futures can offset the loss.

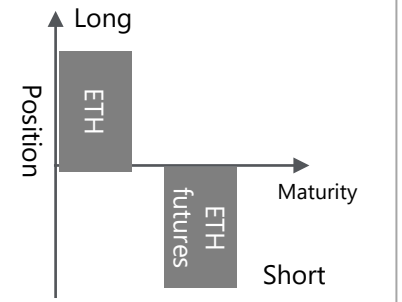
Spread Revenue from Spot-Futures Price Difference

The price of ETH futures tends to be higher than the spot price due to the risk premium associated with future price fluctuations and the supply-demand balance for ETH. By selling futures, it is possible to receive spread revenue.

ETH Price Fluctuations and USDe Revenue

Pattern	Staking Revenue	Backed Asset		Spread Revenue	Total
		ETH	ETH futues		
ETH Price Increase	＋A%	+B%	-B%	+C%	A+C%
ETH Price Decrease	＋A%	−B%	+B%	+C%	A+C%

The impact on collateral value due to ETH price fluctuations is net zero.



The delta position is neutral due to a long position in ETH spot and a short position in ETH futures.

Source: Created by our company based on "Protocol Revenue Explanation" (Ethena Labs) as of February 2025.

Reference: Bank-Issued (EURI)

EURI is the first MiCA-compliant stablecoin issued by an EU bank (Banking Circle), offering "reliability through regulatory compliance" and "safety and efficiency leveraging the strengths of a bank."

Basic Information	
Stablecoin overview	■ The first e-money token issued by Banking Circle and the first MiCA-compliant stablecoin issued and supported by an EU bank. ■ Banking Circle is a payment bank based in Luxembourg and is licensed as a bank in Europe.
Features	■ Reliability: ➢ EURI is fully compliant with MiCA regulations and is audited by top-level auditors to ensure the equivalence between the circulating EURI and the cash received from EURI holders. ■ Safety and Security: ➢ All fiat currency funds received from EURI holders in exchange for EURI are segregated and held as cash or cash equivalents in a bankruptcy-remote structure by Banking Circle. ■ Efficiency: ➢ While converting to fiat currency can be time-consuming and costly, e-money tokens are the smoothest option for fiat currency hedging transactions and can be used for the fast and efficient settlement of other digital currency assets. ■ Redemption at Face Value: ➢ Holders of EURI have the right to redeem at face value at any time, and they can request Banking Circle to redeem (return) EURI at a rate of 1 EUR per 1 EURI at any time.
Situation	■ EURI and Binance have agreed to enable EURI payments on the Binance Pay platform, a cryptocurrency contactless payment technology. This aims to enhance the usefulness of digital currencies in everyday financial transactions.

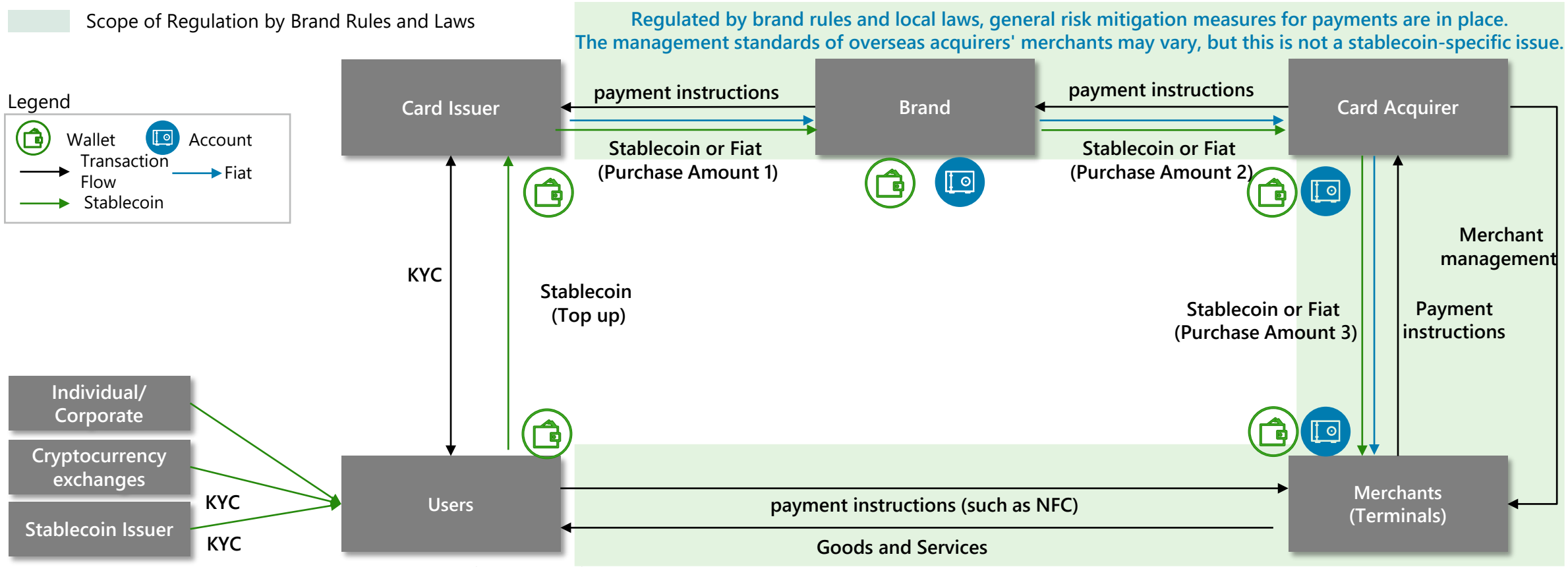
Source: "Banking Circle launches the first bank-backed MiCA-compliant stablecoin, EURI" (BANKING CIRCLE), based on our company's creation, confirmed as of February 2025.

1. Research on Payment-Related Use Cases and Peripheral Services of Stablecoins
1.2 Classification and specific examples of payment-related use cases

Scheme Diagram

Stablecoin holders and merchants looking to reduce payment costs use this service. The payment mechanism follows existing rules, but non-traditional players such as exchanges are responsible for issuing cards.

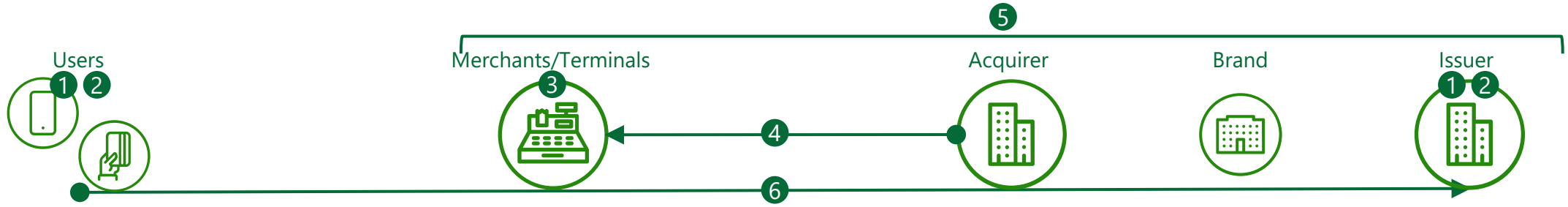
Value Proposition	■ Card Acquirers Reduction in time and cost associated with merchant settlement ■ Card Issuers Provision of fund source options and financial inclusion for the unbanked
Process	■ Users are issued SC-linked credit or debit cards by the card issuer. ■ Based on the user's instruction, the international brand transfers stablecoins or converts them to fiat for the merchant.



*Purchase Amount 1: Purchase amount - Interchange fee + Brand fee (Card Issuer),
Purchase Amount 2: Purchase amount - Interchange fee - Brand fee (Card Acquirer), Purchase Amount 3: Purchase amount - Merchant fee

Reference: Threats and Countermeasures in Existing International Brand Payments

In existing international brand payments, various countermeasures have been implemented to address the threats associated with conducting transactions.



1 Identity Proofing (elimination of high-risk users)

- Implementation is in accordance with laws and regulations.
- In Japan, identity proofing is mandatory for the use of credit and debit cards in accordance with the Act on Prevention of Transfer of Criminal Proceeds.
- It should be noted that the security strength varies depending on the method of identity proofing.

3 Authenticity of Terminals (prevention of terminal tampering, etc.)

- In accordance with brand rules, terminals are certified by EMV and PCI PTS.
  - ✓ EMV Certification: L1 (physical and electrical characteristics), L2 (terminal software) verification.
  - ✓ PCI PTS: Payment Card Industry PIN Transaction Security

5 Proper Management of Credit Card Numbers

- Brand rules and the Installment Sales Act:
  - ✓ Acquirers, issuers, PSP, merchants, and other entities that store or transmit card numbers are required to comply with PCI DSS. Compliance with PCI DSS results in the implementation of advanced security measures, not limited to the handling of card numbers.

2 Cardholder Verification (prevention of impersonation in transactions)

- In-Store Payments
  - ✓ Card possession + PIN or CDCVM or signature*, etc.
    *In Japan, PIN bypass methods will be prohibited.
- E-Commerce payments
  - ✓ EMV 3-D Secure, etc.

4 Merchant Management (Elimination of Malicious Merchants)

- Brand Rules: Establish rules for chargebacks, etc.
- the Installment Sales Act:
  - ✓ In accordance with Japanese regulatory laws, acquirers and PSP are required to be registered. They are required to conduct merchant investigations.

6 Various Authentications During Transactions (Prevention of Message Tampering, etc.)

- Examples of Authentication:
  - ✓ Cardholder Verification (see ❷)
  - ✓ Card Authentication
  - ✓ Transaction Authentication:
    by verifying Message Authentication Codes (MAC) using symmetric key cryptography

References: "the Installment Sales Act"(METI), "Credit Security Guidelines"(JCA), "EMV® Specifications"(EMVCo)

Reference: History of Fraud and Countermeasures in International Brand Payments

As fraud techniques become more sophisticated each year, we need to continuously review our security measures.
Similarly, it is important to ensure security across the entire ecosystem for stablecoins as well.

Typical Fraud Incidents

Counterfeit card fraud

- Damage peaked at 16.5 billion yen in 2002 and has since decreased
  - ➢ Fraud techniques
    - Skimming
    - Modification of payment terminals (insertion of skimming boards and transmitters)
- To reduce damage, IC card implementation is necessary not just in specific countries but at a global.

Card number theft

- 2024 damage amount: 51.35 billion yen *record high
  - ➢ Fraud techniques
    - BIN attack
    - Leakage from businesses
    - Phishing / Real-time phishing
- Fraud techniques are becoming more sophisticated every year, with incidents such as the theft of card information and static passwords during phishing, and the theft of SMS authentication information through SIM swap attack.

International Security Standards

EMVCo: Est. in 1999, operated by Amex, Discover, JCB, Mastercard, UnionPay, and Visa.

- In-Store Payments
  - EMV Specifications: Announced in 1996, these are specifications for the IC cards and terminals are regularly updated.
- E-Commerce payments
  - 3-D Secure 1.0: uses static password authentication.
  - EMV 3-D Secure: utilizes risk-based authentication and recommends dynamic password authentication or biometric authentication.

PCI SSC: The Council was founded in 2006 by Amex, Discover, JCB, Mastercard and Visa.

- PCI DSS: Payment Card Industry Data Security Standard
  - I. Build and Maintain a Secure Network and Systems
  - II. Protect Account Data
  - III. Maintain a Vulnerability Management Program
  - IV. Implement Strong Access Control Measures
  - V. Regularly Monitor and Test Networks
  - VI. Maintain an Information Security Policy
- PCI PTS：Payment Card Industry PIN Transaction Security
- Various standards exist depending on the use case.

Evolution of the Installment Sales Act

Implemented in 2009/2010

➢ Proper Management of Credit Card Numbers was mandated for acquirers and issuers.
(PCI DSS compliant)

Implemented in 2018

➢ The duty of merchant investigation has been imposed on acquirers and others.
➢ Proper Management of Credit Card Numbers was mandated for merchants.

2020

➢ EMV compliance deadline for cards and terminals.
Reference: Liability shift as a brand rule began in 2015, increasing the motivation for compliance from a business perspective.

Scheduled for 2025

➢ EMV 3-D Secure Compliance Completion Target for E-Commerce Sites.
Reference: In the EU, PSD2 SCA has been mandated since 2019, and 3-D Secure has been advanced as a compliance measure.

References: "the Installment Sales Act"(METI), "Credit Security Guidelines" "The Incidence of Credit Card Fraud"(JCA), "EMV® Specifications"(EMVCo)

Case Study

Lemon Card, in collaboration with Visa, offers a prepaid card that enables cryptocurrency payments at Visa-affiliated merchants. Similarly, Fiat24, in partnership with SafePal, provides a Visa card that allows cryptocurrency payments.

（Case Study） Lemon

Basic Information			
Stablecoins	USDT/USDC/DAI	**Year in Service（SC payment）**	After 2021
Business Operator	Lemon（Argentina）	**Jurisdiction**	Argentina

Service Overview	
Service Details	➢ Lemon, in cooperation with Visa, offers the Visa Lemon Card, which enables cryptocurrency payments at Visa-affiliated merchants. ➢ Lemon provides users with a card that allows cryptocurrency payments, and Visa integrates a system into its branded payment network that enables settlements in USDC and USDT. This system allows payments not only in USDT and USDC but also in BTC, ETH, DAI, and Argentine Pesos. ➢ Users can receive up to 2% cashback in BTC when using this card. As of January 2024, over one million cards have been issued, and there are more than three million app users.
Business Scale	➢ As of January 2024, over one million cards have been issued, and there are more than three million app users.
Notes	➢ To apply for the card, the following requirements must be met: • Be at least 18 years old and complete the standard identity verification process (ID card, selfie photo, email). • Be a resident of Argentina (U.S. citizens are not accepted even if they are residents). • Provide the user's CVU (e.g., MercadoPago) and CBU (user's bank account).

[References]：「Get Your Crypto Card: Earn Bitcoin for Using It」（Lemon） as of March 2025

（Case Study） Fiat24

Basic Information			
Stablecoins	USDC	**Year in Service（SC payment）**	2024
Business Operator	Fiat24（Swisse）	**Jurisdiction**	30 European countries

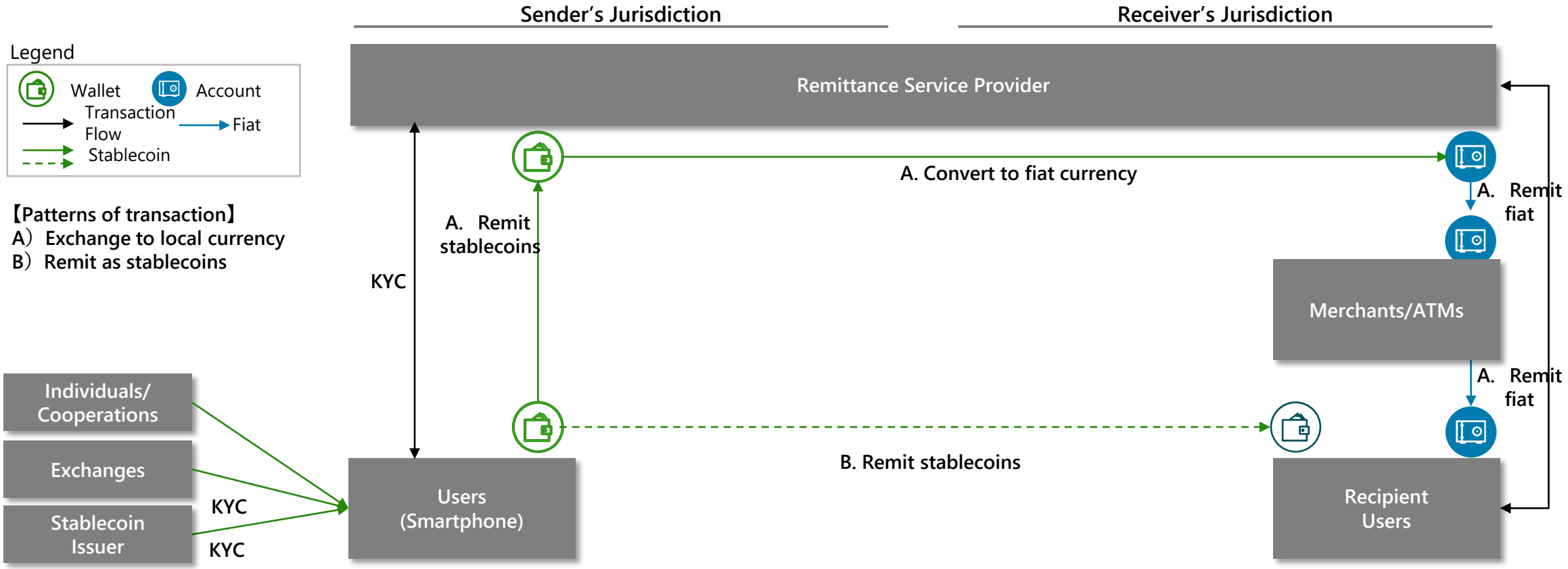
Service Overview	
Service Details	➢ Fiat24, in collaboration with SafePal, offers a Visa card that enables cryptocurrency payments at Visa-affiliated merchants ➢ Fiat24 provides users with a card that allows cryptocurrency payments, and Visa integrates a system into its branded payment network that enables settlements in USDC. ➢ There are no issuance fees or monthly charges for the card, and the monthly usage limit is set at 10,000 euros.
Business Scale	➢ The card can be used at over 40 million merchants worldwide as of January 2025.
Notes	➢ It complies with Swiss banking laws, anti-money laundering regulations, and sanction regulations. ➢ The card issuance is available to individuals aged 18 or older residing in EEA member countries or Switzerland, and identity verification is conducted using a passport or biometric ID ➢ Additionally, location information is required to confirm residency in the target country during account registration.

[References]：「Stay tuned of the latest updates and announcements of SafePal」（SafePal） as of March 2025

Scheme Diagram

It is utilized as a means of transferring funds to the unbanked or underbanked populations, and while payment intermediaries comply with the regulations of each jurisdiction, the strength of these regulations may vary by country or region.

Value Proposition	Process
■ User 1: Reduction in time and cost associated with cross-border remittances ■ User 2: Financial inclusion for the unbanked or underbanked populations	■ Based on the user's instruction for an SC payment, the remittance network operator exchanges the SC for fiat currency and then transfers it to the receiver. ■ Alternatively, the user may directly send the SC to the receiver.



Case Study

Yellow Card provides remittance services using stablecoins to people in Africa who have unstable local currencies or insufficient access to financial services, and Coins.ph offers similar services.

（Case Study） Yellow Card

Basic Information			
Stablecoins	USDT/USDC/PYUSD	**Year in Service（SC payment）**	2024
Business Operator	Yello Card（South Africa）	**Jurisdiction**	30 African countries

Service Overview	
Service Details	➢ Yellow Card offers free instant stablecoin transfer services through Yellow Pay. ➢ They aim to provide simple and fast transfers through an excellent UI, with no fees for sending and depositing, while withdrawals incur a fee of 100 NGN (Nigeria). ➢ Incentives are provided through referral programs, ambassador programs, and bug bounty programs. Referring a friend allows you to receive 20% of the transaction fees from the referred friend.
Business Scale	➢ They operate in 20 African countries and have acquired 1.7 million customers by 2023.
Notes	➢ KYC requires the registration of personal information, and the upload of identification documents and a selfie.

[Reference] ：「Buy and Sell BTC, ETH, USDT & More in Africa」（Yellow Card） as of March 2025

（Case Study） Coins.ph

Basic Information			
Stablecoins	USDC	**Year in Service（SC payment）**	2023
Business Operator	Coins.ph（Philippines）	**Jurisdiction**	Philippines

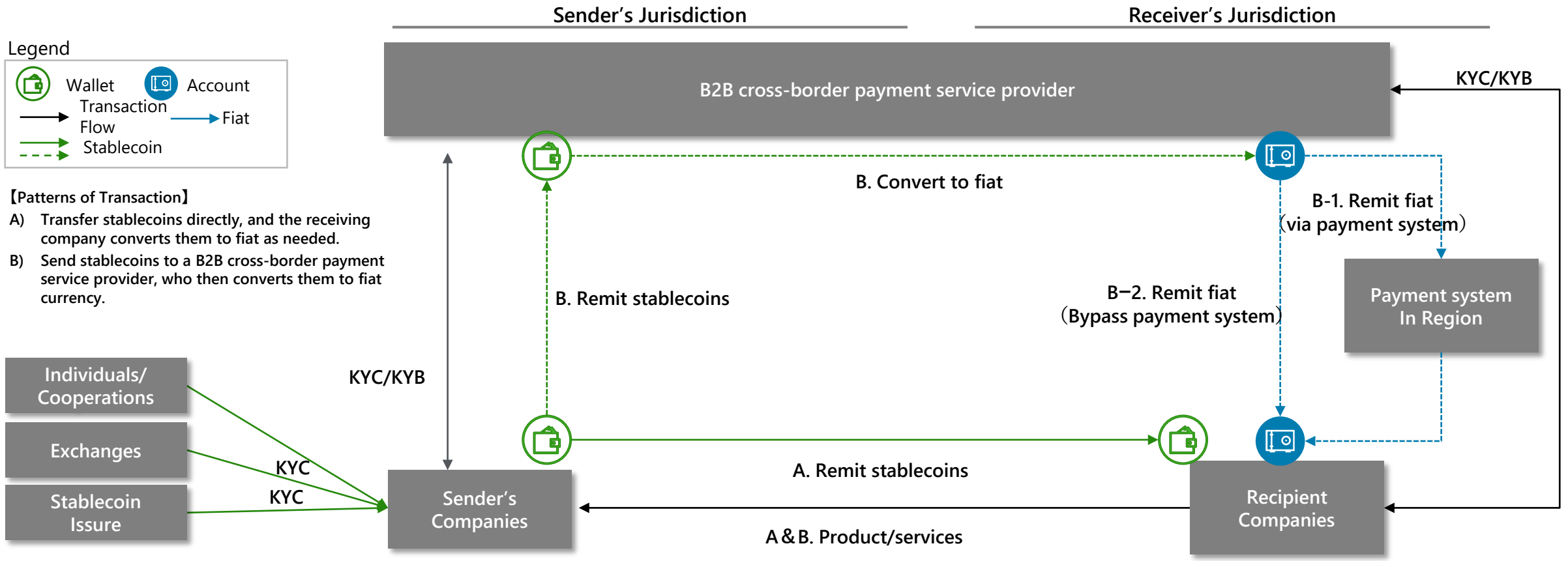
Service Overview	
Service Details	➢ Coins.ph offers international remittance solutions using USDC for Filipino users, allowing withdrawals at over 100 banks and pawnshops through the Coins.ph app. ➢ Coins.ph exchanges USDC/USDT received from users into fiat and transfers it to the recipient's bank account. ➢ The bug bounty program offers rewards ranging from $10 to $5,000 for reporting vulnerabilities.
Business Scale	➢ They have over 16 million registered users (as of January 2025).
Notes	➢ They have obtained Virtual Currency and Electronic Money Issuer licenses from BSP. ➢ Account creation is targeted at individuals aged 18 and over, with KYC conducted based on a selfie and identification documents such as a passport or driver's license.

[Reference] ：「Trusted Crypto Wallet & Exchange | Buy Bitcoin in the Philippines」（Coins.ph） as of March 2025

Scheme Diagram

The use of stablecoins as a rapid and low-cost payment method has become widespread. However, there have also been transactions aimed at evading sanctions and capital controls, necessitating the development of measures against illicit activities, such as freezing targeted addresses.

Value Proposition	Process
■ Companies: Reduction in time and cost associated with cross-border remittances	■ Based on the instruction for SC payment from a company at the time of purchasing goods or services, the B2B cross-border payment service provider exchanges the SC for fiat currency and then transfers it to the receiver. ■ Alternatively, the company may directly send SC to the recipient company for payment.



Case Study

Circle (USDC) collaborates with PIX to enable instant and low-cost cross-border transactions, and BVNK provides a payment platform that allows businesses to settle transactions using stablecoins.

（Case Study） PIX

Basic Information			
Stablecoins	USDC	Year in Service（SC payment）	2024
Business Operator	Circle（US）/ PIX（Brazial）	Jurisdiction	Brazil

Service Overview	
Service Details	➢ Brazil's real-time payment system, PIX, in collaboration with Circle, enables immediate and low-cost cross-border transactions by allowing recipient companies to instantly exchange USDC and fiat currency. ➢ For fiat transactions, PIX payments are settled in an average of 3 seconds. It is mandated to be free for individuals. The cost for corporate/merchant payment transactions is 0.33% of the transaction amount. ➢ (Reference) Circle also supports local bank transfers through Mexico's national real-time payment system, SPEI.
Business Scale	➢ Since its release, PIX has been used by over 140 million individuals and 13 million companies (as of May 2023)
Notes	➢ Participants in the system are subject to regulatory requirements by the Central Bank of Brazil (BCB). • They are subject to basic regulations concerning risk-based supervision, liquidity risk management, cybersecurity, data usage, and AML/CFT procedures. ➢ To comply with KYC rules, participants must flag suspicious transactions and assign transaction limits according to the user's risk profile.

[Reference]「USDC now available in Brazil and Mexico」（Circle） as of March, 2025
「Pix: Brazil's Successful Instant Payment System in: IMF Staff Country Reports Volume 2023 Issue 289 (2023)」
（IMF eLIBRARY） as of March, 2025

（Case Study） BVNK

Basic Information			
Stablecoins	USDT/USDC/ PYUSD	Year in Service（SC payment）	2024
Business Operator	UK	Jurisdiction	US/UK/Europe

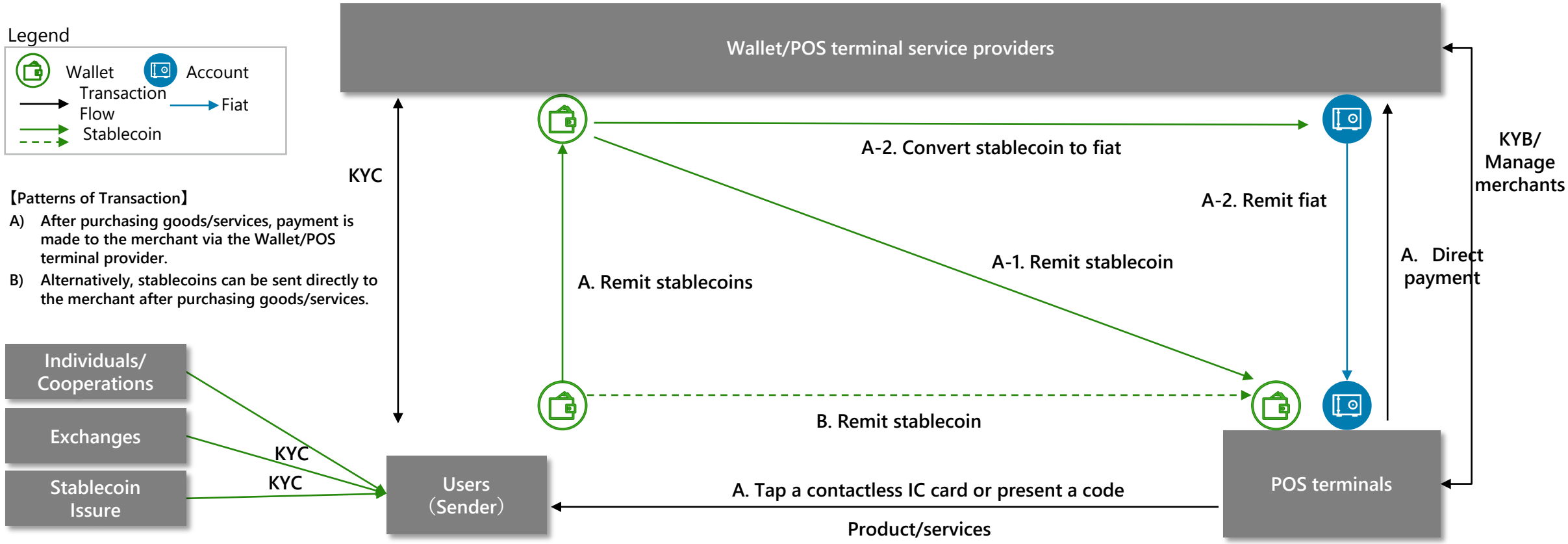
Service Overview	
Service Details	➢ BVNK provides a payment platform that enables businesses to quickly and securely send, receive, and exchange stablecoins with fiat currencies. ➢ It is also possible to convert stablecoins to fiat and send them to recipient companies, primarily supporting EUR, GBP, and USD. ➢ For AML and KYC, we deploy a combination of tools and proprietary machine learning models to effectively detect and prevent crimes, helping to mitigate financial crime risks.
Business Scale	➢ BVNK processes over $12 billion in payments annually, achieving a 200% year-on-year growth as of February 2025.
Notes	➢ BVNK is regulated as an EMI in the UK and Europe and holds multiple VASP registrations in Europe. ➢ In the United States, our entity established in Delaware holds money transmitter licenses in several states and is registered with FinCEN (Financial Crimes Enforcement Network of the U.S. Department of the Treasury).

[Reference] ：「Trusted Crypto Wallet & Exchange | Buy Bitcoin in the Philippines」（Coins.ph） as of March 2025

Scheme Diagram (Case of Proprietary Rails Other Than International Brands)

Stablecoins are used for everyday in-store payments by users and merchants who prefer them. Due to the proprietary rails of the payment system, this scheme allows for unique handling by service providers, including authentication and other general processes.

Value Proposition	■ Store: Reduce settlement time and various costs of existing payment rails ■ User: Provide options for fund sources, financial inclusion for those who cannot open bank accounts
Process	■ After purchasing goods or services, the user sends SC in advance to the address of the Wallet/POS terminal provider based on the payment instruction from the user, and then sends SC to the store ■ Alternatively, the user directly sends SC to the store for payment



Case Study

We provide POS terminals and card devices with proprietary rails that support the exchange of payment messages using stablecoins (including other cryptocurrencies), enabling stablecoin payments at physical stores.

（Case Study） Pundi X

Basic Information			
Stablecoins	USDT/DAI	**Year in Service（SC payment）**	2022
Business Operator	Pundi X (Singapore)	**Jurisdiction**	Over 30 countries

Service Overview	
Service Details	➢ Payment for purchases with USDT or DAI is possible through XPOS installed in stores (cryptocurrencies like BTC are also supported, and USDT or DAI can be purchased through the store's XPOS). ➢ Users can use wallets like MetaMask or f(x)wallet, and if they prefer physical cards, they can purchase and use p(x)Card. ➢ XPOS is installed on terminals from vendors such as Verifone, Ingenico, and PAX, and sold to stores, which then link f(x)wallet to XPOS.
Business Scale	➢ XPOS and p(X)Card are sold in over 30 countries worldwide, including Japan. A list of stores where they can be used in Japan has also been published.
Notes	➢ Although the terminals are manufactured by terminal vendors that sell EMV-certified terminals, the applications installed on them are independently developed by Pundi X.

[Reference] ：「Pundi X Official 、Function X」（Function X） _as of March, 2025

（Case Study） dtcpay

Basic Information			
Stablecoins	USDT/USDC/WUDS	**Year in Service（SC payment）**	2024
Business Operator	dtcpay（Singapore）	**Jurisdiction**	Singapore

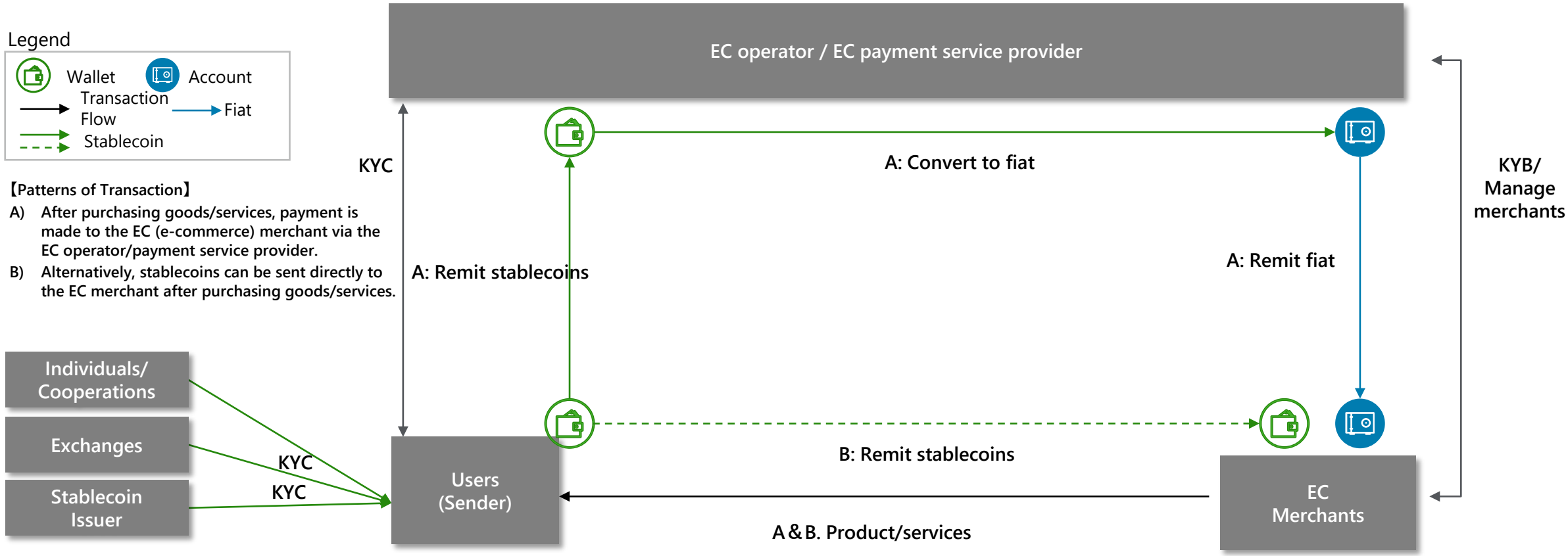
Service Overview	
Service Details	➢ dtcpay offers POS+ systems that can accept stablecoin payments in addition to traditional payment methods such as credit cards. ➢ At merchants that have implemented POS+, users can make payments using stablecoins. ➢ When stablecoins are selected as the payment method, transaction fees can be kept lower compared to traditional payment methods.
Business Scale	➢ The number of companies that have adopted the system is unknown, but it is being implemented in industries such as retail and travel.
Notes	➢ It supports payments with stablecoins, electronic money, and credit cards, and can also manage transaction histories. ➢ It complies with PCI DSS requirements, encrypting and storing card data.

[Reference] ：「Point of Sale Solutions」（dtcpay） _as of March, 2025

Scheme Diagram

The initiative to allow the selection of stablecoins as a payment method when purchasing goods on e-commerce platforms is increasing. To prevent illicit activities, it is crucial for EC operators and payment service providers to establish robust risk mitigation measures, including Know Your Customer (KYC) protocols for users.

Value Proposition	■ Stores: Reduction in settlement time and various costs associated with existing payment rails ■ Users: Provision of options for funding sources, financial inclusion for individuals unable to open bank accounts
Process	■ Based on the instruction for SC (stablecoin) payment from a company at the time of purchasing goods or services, the B2B cross-border payment service provider exchanges the SC for fiat currency and then transfers it to the receiver. ■ Alternatively, the company may directly send SC to the recipient company for payment.



Case Study

Stripe has enabled the option to select USDC as a payment method when purchasing products on e-commerce platforms. Additionally, Grab offers stablecoin payment services to GrabPay users.

（Case Study） Stripe

Basic Information			
Stablecoins	USDC	**Year in Service（SC payment）**	2024
Business Operator	Stripe	**Jurisdiction**	US

Service Overview	
Service Details	➢ Stripe has re-enabled cryptocurrency payments for US companies, offering services that accept USDC via Ethereum, Solana, and Polygon. ➢ When purchasing goods on e-commerce sites, users can link their wallets and sign transactions to send USDC from their wallets to complete the payment. Specifically, by setting "Pay with Crypto," an option to select cryptocurrency as a payment method will appear on the payment form. ➢ The transaction limit is $10,000 per transaction and $100,000 per month, with a transaction fee of 1.5% of the transaction amount.
Business Scale	➢ As of January 2025, it is only available to a limited number of companies in the US, but Stripe currently supports 46 countries, and the number of supported countries is expected to increase.
Notes	➢ The total payment volume processed by all businesses using Stripe reached the $1 trillion mark in 2023, a 25% increase from the previous year.

[Reference]: " https://docs.stripe.com/crypto/pay-with-crypto ", " https://stripe.com/jp/global ", "Stripe_2023_annual_letter_JA.pdf" (Stripe) as of March 2025.

（Case Study） Grab

Basic Information			
Stablecoins	USDT/USDC/XSGD	**Year in Service（SC payment）**	2024
Business Operator	Grab（Singapore）	**Jurisdiction**	Singapore

Service Overview	
Service Details	➢ Grab provides stablecoin payment services to GrabPay users, which can be used for online shopping, taxi fares, and other Grab services, as well as for e-commerce and in-store payments. ➢ Currently, the service is only available in Singapore, but there are plans to expand based on demand. Transfers can be made instantly without fees, and transaction histories can be checked.
Business Scale	➢ Grab has over 180 million users (as of 2023). ➢ GrabPay has over 100 million users (as of 2023).
Notes	➢ It complies with PCI DSS, boasting a high level of security. ➢ Payments made using GrabPay can earn up to 0.5% cashback in GrabRewards points, and as long as GrabPay is used regularly, the points do not expire.

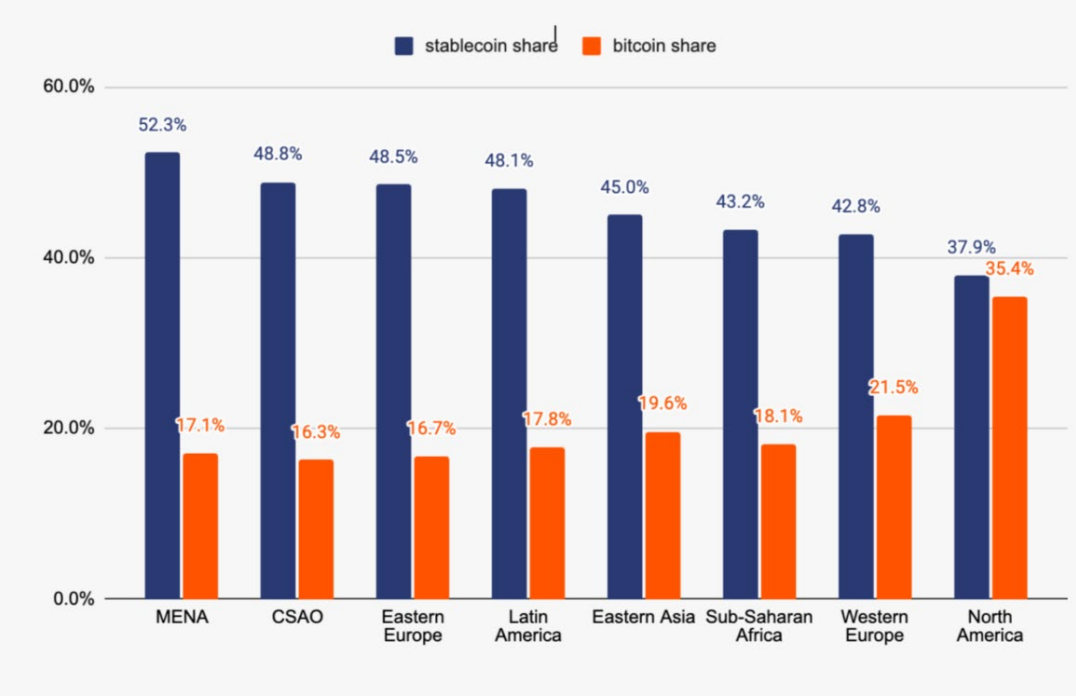
[Reference]：「GrabPay - Mobile Wallet Payment Solution | Grab PH」（Grab）_as of March 2025

1. Investigation of Payment-Related Use Cases and Peripheral Services for Stablecoins
1.3 Technologies and Services that Promote Adoption

Stablecoin Adoption Status

In jurisdictions with high inflation rates and unstable fiat currency prices, or where bank account ownership rates are low, the adoption of stablecoins is reported to be advancing.

Share of stablecoins in cryptocurrencies (by region, repeated) ※1



*1 Regional statistics are calculated by allocating values based on the countries accessing the exchanges using traffic data.

■ In regions such as MENA, CSAO, Eastern Europe, and Latin America, where many countries have unstable or highly volatile fiat currencies, the use of stablecoins as a reliable means of payment and value storage is high.

Share by coin and inflation/bank account ownership rates ※1･4

		BTC	ETH	Alt-coins	stablecoins	Infraition rate※2	Account ownership ※3
North America	Canada	23.7%	8.4%	26.8%	41.1%	3.35%	—
	US	37.0%	6.8%	18.7%	37.5%	3.97%	95.0%
	Balmuda	11.9%	4.1%	38.8%	45.2%	—	—
Latin America	Argentina	14.7%	10.0%	13.4%	61.8%	69.98%	66.3%
	Brazil	14.2%	12.1%	13.8%	59.8%	5.82%	83.6%
	Columbia	13.7%	8.8%	11.5%	66.0%	6.29%	55.9%
	Mexico	19.3%	16.6%	17.0%	47.2%	5.23%	49.1%
	Venezuela	12.2%	15.9%	15.4%	56.4%	4,874.00%	—
MENA	Israel	19.9%	7.3%	32.3%	40.6%	2.07%	—
	Saudi Arabia	16.4%	7.8%	29.7%	46.1%	1.84%	—
	Türkiye	15.6%	8.5%	20.7%	55.2%	34.65%	73.4%
	UAE	16.5%	7.8%	24.4%	51.3%	0.47%	—
whole world		**22.3%**	**8.3%**	**24.6%**	**44.7%**	**5.34%**	**74.0%**

※2 Average consumer price inflation rate over the past 5 years (2019-2023)
※3 Bank account ownership rate as of 2021
※4 Data compiled from countries for which data is available from the source

■ There is a positive correlation between the share of stablecoin holdings and inflation rates. In countries with high inflation rates, such as Argentina and Venezuela, the proportion of stablecoin holdings is high.

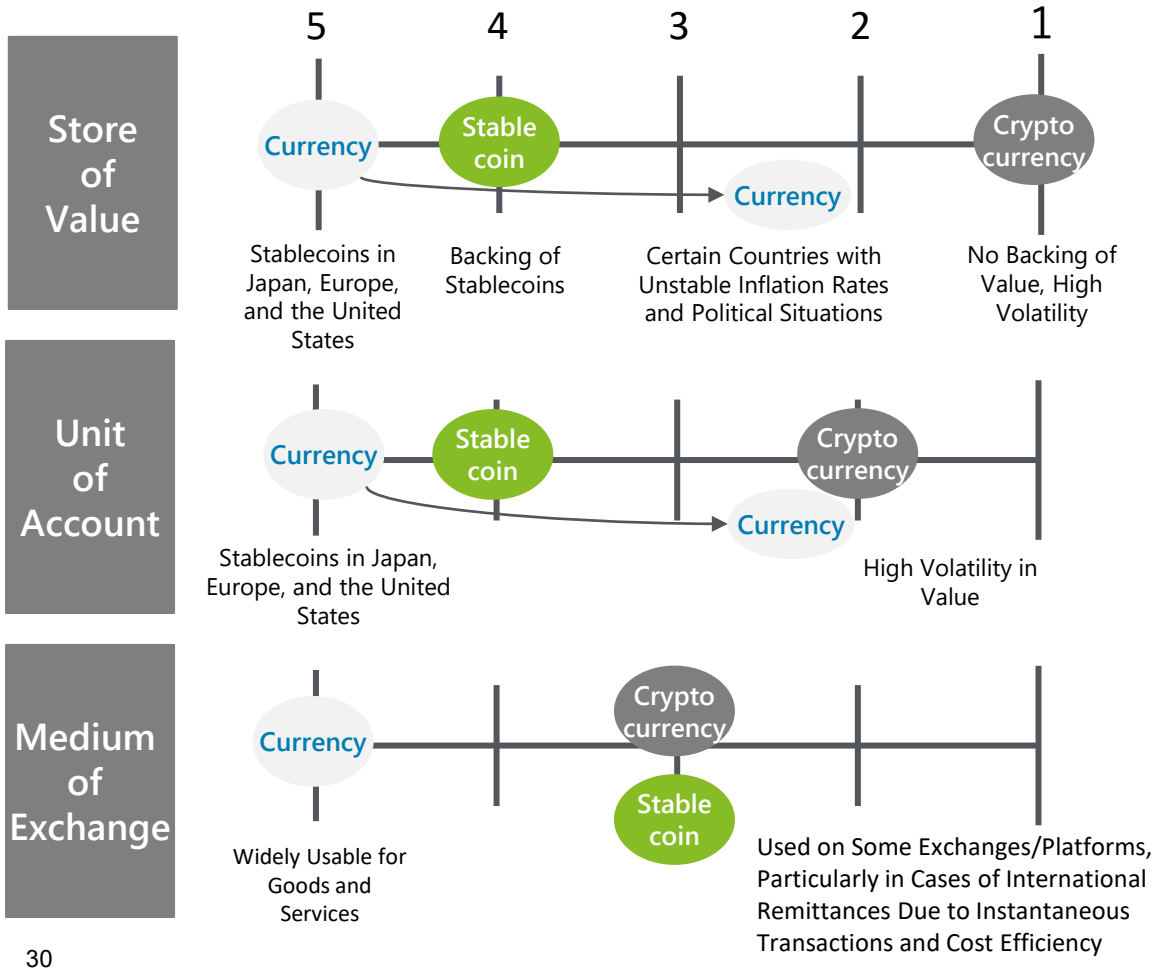
Source: Created by our company based on "The 2024 Geography of Crypto Report" (Chainalysis) as of March 2025

References: " https://www.jetro.go.jp/biz/areareports/2022/82df5175afac50a6.html " (JETRO, Bank Account Ownership Rates) " https://www.globalnote.jp/" (Globalnote, Consumer Price Inflation Rates) as of March 2025

Factors Contributing to the Adoption of Stablecoins

In some jurisdictions, stablecoins fulfill the basic functions of currency ("store of value," "unit of account," and "medium of exchange") better than the local currency, contributing to their widespread adoption. Cryptocurrencies, however, face challenges due to their value volatility.

The Degree of Fulfillment of Basic Currency Functions by Traditional Currency, Stablecoins, and Cryptocurrencies



Factors Contributing to the Adoption of Stablecoins

- Store of Value as a Substitute for Local Currency in Certain Countries
- Integration with Existing Payment Networks
- Faster Transfer Speeds and Lower Fees Compared to Traditional Currency

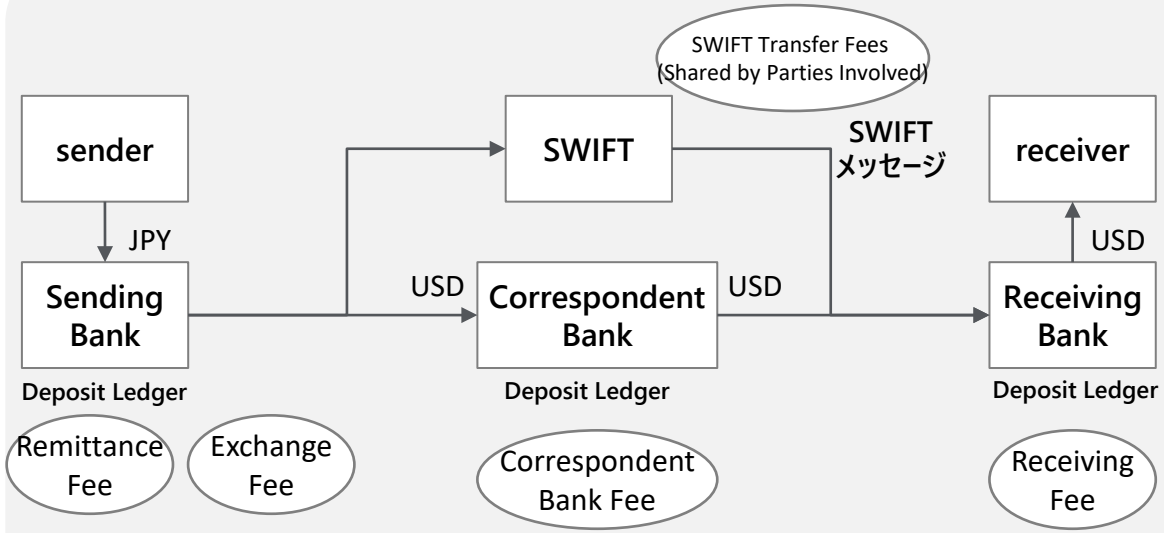
Reference: Technologies that Promote Adoption (Cross-border Payments/Remittances)

Traditional payment methods incur high costs due to the involvement of numerous intermediaries such as financial institutions. However, stablecoin payments utilizing blockchain technology enable peer-to-peer (P2P) transactions, thereby reducing costs.

Traditional Payment Process

■ Due to the presence of numerous intermediary institutions and systems, remittances take time and incur high costs.

International Remittance

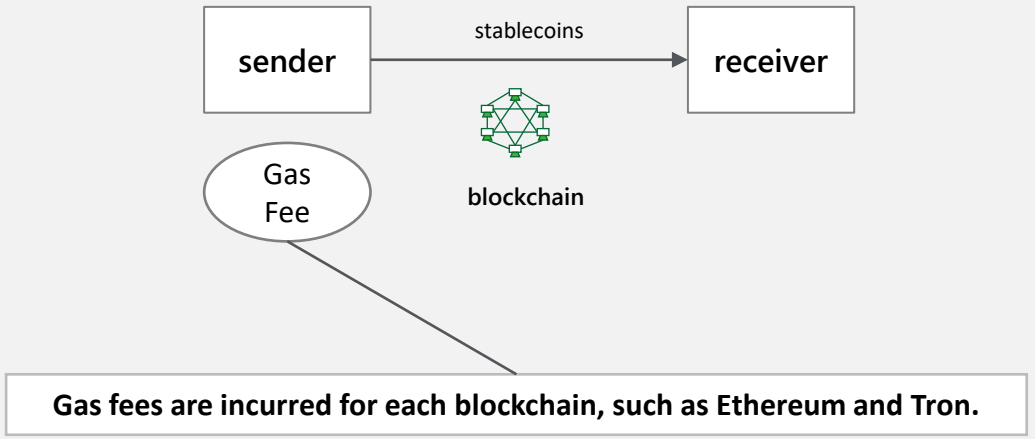


- In the case of international remittances, the total cost of the remittance fee, correspondent bank fee, and receiving fee is approximately 10,000 yen.
- Additionally, an exchange fee based on the remittance amount and the fee rate for different currencies will incur as a cost. Generally, international remittances take several days to about a week.

Stablecoin Payment Process

■ Since peer-to-peer (P2P) transactions are realized on the blockchain, the time required for remittances is short and the costs are low.

Stablecoin Payment



- Even for international remittances, the main cost incurred is only the gas fee, and since the transfer is made directly from the wallet, the remittance is completed in a short time.

2. Research on Illicit Use of Stablecoins

2.1 Overview: Definition and Categorization of Illicit Use

Overview - Illicit Use

In this research, "Illicit use" is defined as the use of crypto ecosystem that results in unjust consequences for legitimate users, or by who are sanctioned.

Definition of illicit use in this report

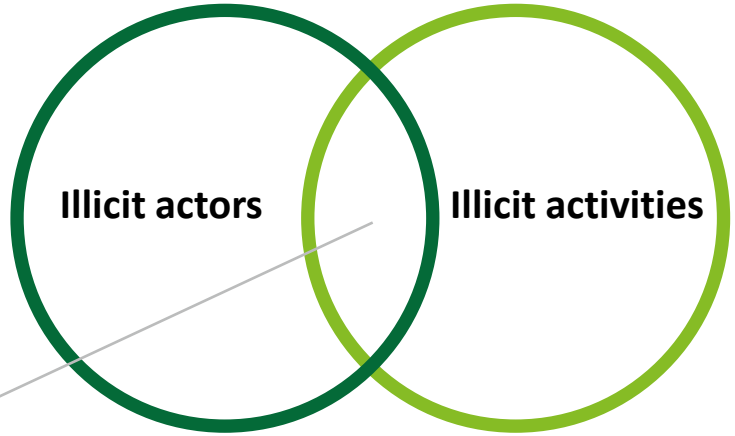
- In this research, "Illicit use" refers to **(1) the use of crypto ecosystem for criminal activities, etc. that results in unjust consequences for any legitimate user in terms of social conventions, or (2) the use of crypto ecosystem by sanctioned persons (individuals / entities / organizations) or persons in sanctioned jurisdictions (countries / regions), which have been deemed unjust from the perspective of certain sovereignties.**
- It should be noted that the “perspective of certain sovereignties" in (2) is relative, as what is considered “unjust” from one sovereignty’s perspective may not be seen as such from another.

Focus of this report

- The above defined illicit use encompasses (i) the inflow of funds by conducting scams or hackings, and (ii) the subsequent laundering process and cashing out of those funds. This report focuses on analyzing (ii).
- That is, it should be noted that, this report does not address large-scale hacking incidents that result in significant outflows from cryptocurrency exchanges (the abovementioned (i)).

Categorization of illicit use

- While various attempts have been made to categorize illicit use, from the perspective of **how illicit use are identified**, generally it can be classified into the following two groups:
  - ✓ **Those identified by detecting illicit actors**
  - ✓ **Those identified by detecting illicit activities**
- **There can be overlap between the two groups**, such as cases in which the illicit activity is firstly detected and later the persons who did it are identified.

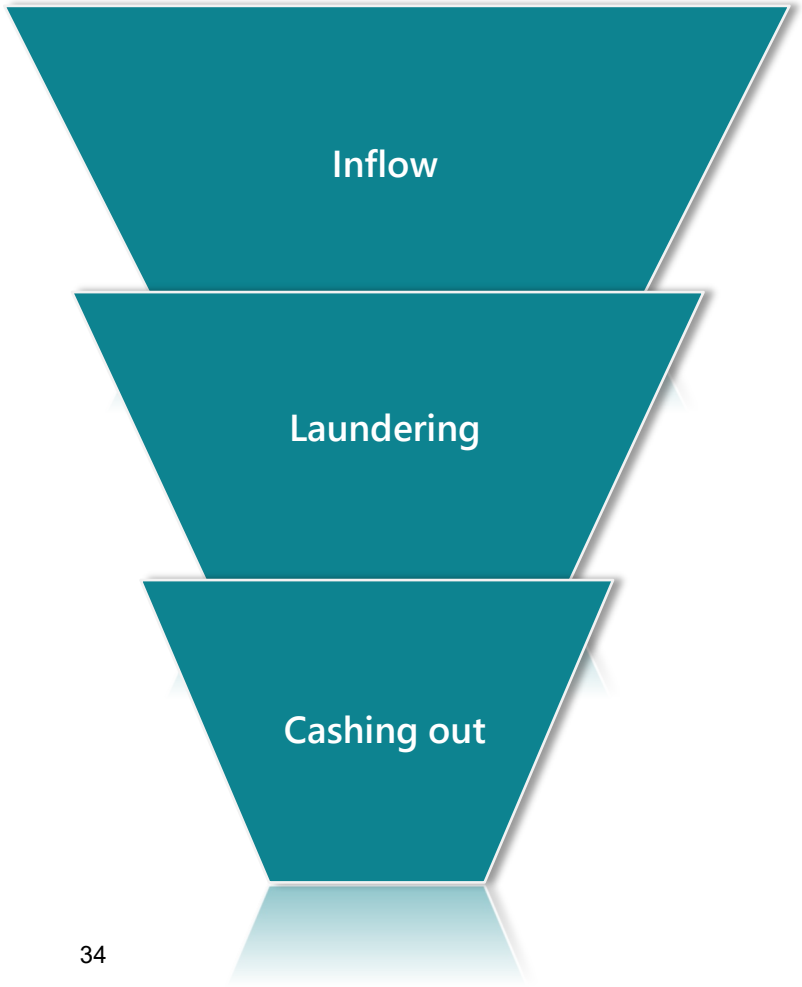


An example: A hacking attack has been detected and a crypto address involved in it may later be identified as belonging to a specific criminal organization, and all the transactions from/to that address may subsequently be tagged as ‘illicit’.

Three steps of illicit use

The process of blockchain illicit use has three steps: inflow, laundering, and cashing out. It is necessary to analyze the characteristics and countermeasures at each stage.

[Premise] : **Due to the high interchangeability of stablecoins with crypto-assets**, even if measures to prevent illicit use in the issuance and circulation of stablecoins are established, these measures could be circumvented through exchanges with crypto-assets.



	Description
Step1	■ Activities of accumulation of tokens from crimes such as hackings and scams at specific addresses on the blockchain • Activities involving **thefts of tokens** using off-chain tools such as websites and social medias, **payments for ransomware or transactions on the dark web**, **tax evasion concealment**, etc. • Activities involving fund transfers from clean addresses to sanctioned addresses.
Step2	■ Activities aim at disrupting tracking by moving tokens using on-chain laundering techniques • Activities involving the use of mixing/tumbling services, privacy coins, dapps, DeFi, etc. to launder funds.
Step3	■ Activities of moving funds to an endpoint such as exchanges and cashing out into fiat currency • Activities involving the use of off-ramp services in jurisdictions with lax AML/CFT regulations or knowingly cashing out illicit funds.

Categorization of illicit use based on cryptocurrency crime reports by analysis tool vendors (1/2)

The increasing proportions of stablecoins in illicit use and the sophistication of cryptocurrency-related criminal activities have been observed.

- Both Chainalysis and TRM Labs have estimated the volume of funds sent to illicit addresses identified and funds stolen through hackings, categorized cryptocurrency-related criminal activities with similar structures shown as 'Category level 2' in the table below.
- The table below groups the categories into "① Identified by detecting illicit actors (subject to sanctions)" and "② Identified by detecting illicit activities (causing financial damage to legitimate parties)", summarizes the volume estimates, trends, and challenges in risk prevention from both companies' reports.

Category level 1	Category level 2	Definition	FY2023 Estimates (Unit: 100M USD)		Trend	Challenges in risk prevention
			Chainalysis	TRM labs		
① **Identified by detecting illicit actors** (Subject to sanctions)	**Sanctions**	Funds sent to cryptocurrency addresses that belong to sanctioned persons (individuals / entities / organizations) or persons in sanctioned jurisdictions (countries / regions) by OFAC, etc.	149	162	■ Shift to stablecoins (approximately 80%) *1 ■ While OFAC sanctions lists are getting longer, the volume of this category decreased *1*2	■ Laundering techniques involving collaboration with mixers and ransomware groups *1*2 ■ Evasion of sanctions through decentralized operations by malicious mixers *1
	Terrorist financing	Funds sent to cryptocurrency addresses related to terrorists	No breakdown data	No breakdown data	■ Hezbollah's expanding of its financial infrastructure into cryptocurrencies involves complex financial networks using various intermediary services *1 ■ There are cases of abuse of cloud-funding and donations *1 ■ High proportion of small amount transfers *1*2 ■ Significant increase in the use of Tether (USDT) *2	■ The complexity of verifying activities related to terrorism in both cash and cryptocurrencies *1 ■ For terrorists have complex financial networks using various intermediary services, it is challenging to distinguish them from legitimate users and humanitarian aid by analyzing only on-chain data *1
	Money laundering of other criminal proceeds	Funds sent to cryptocurrency addresses that belong to ransomware groups, cybercrime organizations, etc.	>11	No breakdown data	■ Regarding the destination of ransomware funds, centralized exchanges and mixers consistently account for a large portion, but there is a high concentration and increase in amounts towards new laundering services (bridges, instant exchangers, gambling services, etc.) *1 ■ While the use of illicit services is dropping, the proportion of illicit funds sent to DeFi protocols increased *1 ■ Off-ramp to fiat currency has high concentration in specific services *1	■ The possibility of a wider scope of money laundering activities through more nested services and addresses *1 ■ Sophisticated techniques that abuse bridges and mixers *1

[Source]: "The 2024 Crypto Crime Report" (Chainalysis, April 2024) *1, "The Illicit Crypto Economy - Key Trends from 2023" (TRM Labs, April 2024) *2 _March 2025

Categorization of illicit use based on cryptocurrency crime reports by analysis tool vendors (2/2)

The increasing proportions of stablecoins in illicit use and the sophistication of cryptocurrency-related criminal activities have been observed.

- Both Chainalysis and TRM Labs have estimated the volume of funds sent to illicit addresses identified and funds stolen through hackings, categorized cryptocurrency-related criminal activities with similar structures shown as 'Category level 2' in the table below.
- The table below groups the categories into "① Identified by detecting illicit actors (subject to sanctions)" and "② Identified by detecting illicit activities (causing financial damage to legitimate parties)", summarizes the volume estimations, trends, and challenges in risk prevention from both companies' reports.

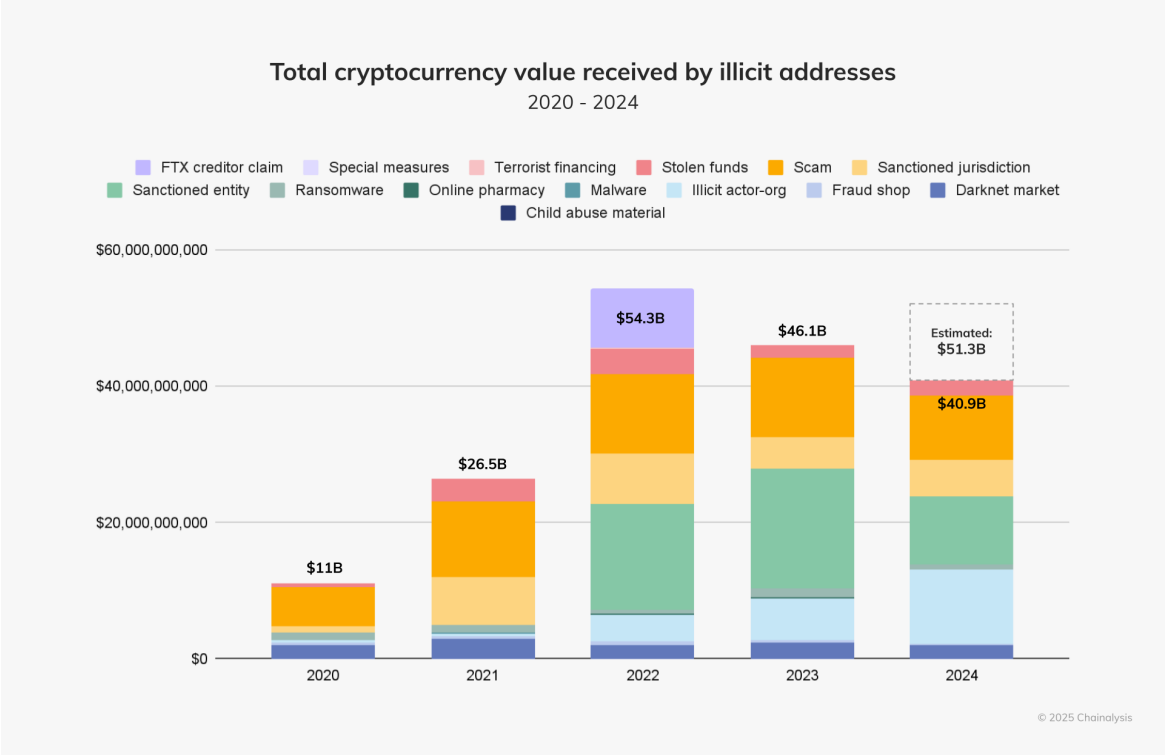
Category level 1	Category level 2	Definition	FY2023 Estimates (Unit: 100M USD)		Trend	Challenges in risk prevention
			Chainalysis	TRM labs		
② **Identified by detecting illicit activities** (Causing financial damage to legitimate parties)	**Stolen funds**	Funds stolen through cryptocurrency hackings	17	18	■ Increasing use of stablecoins (over 30%) *1 ■ Stolen funds decreased by more than 50% from previous year, but the number of hackings slightly increased *1*2 ■ Infrastructure attacks such as theft or leakage of private keys and seed phrases significantly increased (approximately 60%) *2 ■ Decrease in DeFi hacking, but several large-scale hacks occurred *1	■ Both on-chain and off-chain vulnerabilities, particularly the leakage of private keys, price manipulation hacks, and the exploitation of smart contracts, have been contributing factors to hacking incidents *1
	Scams	Funds sent to cryptocurrency addresses associated with scams	46 (※)	125	■ Shift to stablecoins (approximately 70%) *1 ■ The overall volume of this category has decreased, but scam tactics have become more sophisticated and diverse *1*2	■ In romance scams, etc., victims are targeted to build a relationship with the scammer before the final execution, making it difficult to detect in many cases *1 ■ Approval phishing scams show different patterns in on-chain operations compared to many other types of scams, making it difficult to capture all the related activities *1
	Others	Transactions involving illegal pharmacies, darknet market, etc.	>17	>16	■ Some darknet markets and websites that sell illegal data have started integrating their websites with cryptocurrency payment service providers via APIs *1	■ –
		(Total for ①+②)	242	349		

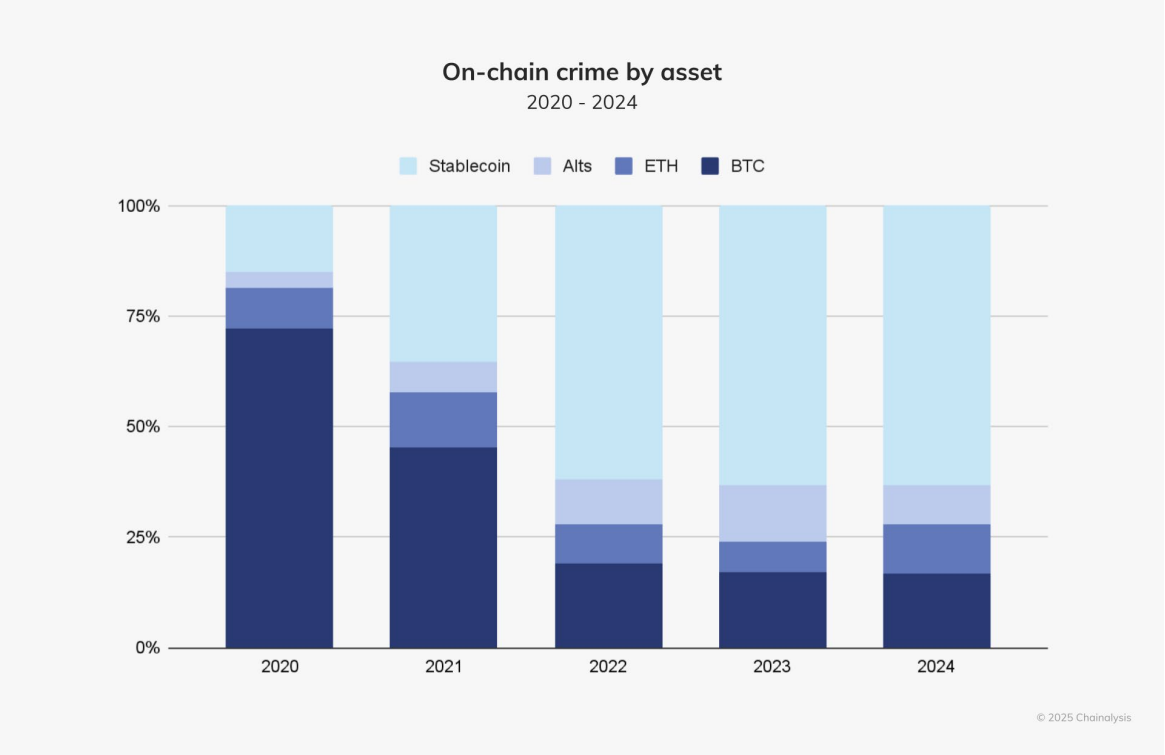
(※) The scam estimate by Chainalysis does not include cases where scammers claim to be promoting a cryptocurrency investment opportunity but receive funds from victims in fiat currency.

[Source]: "The 2024 Crypto Crime Report" (Chainalysis, April 2024) *1, "The Illicit Crypto Economy - Key Trends from 2023" (TRM Labs, April 2024) *2 _March 2025

Latest Crypto Crime Trends

In recent years, the high usage rate of stablecoins in Sanctions related area, which accounts for the highest proportion out of total illicit volume, resulting in stablecoins becoming the most illicitly used crypto currency when analyze the total illicit volume.





2025 Crypto Crime Trends:

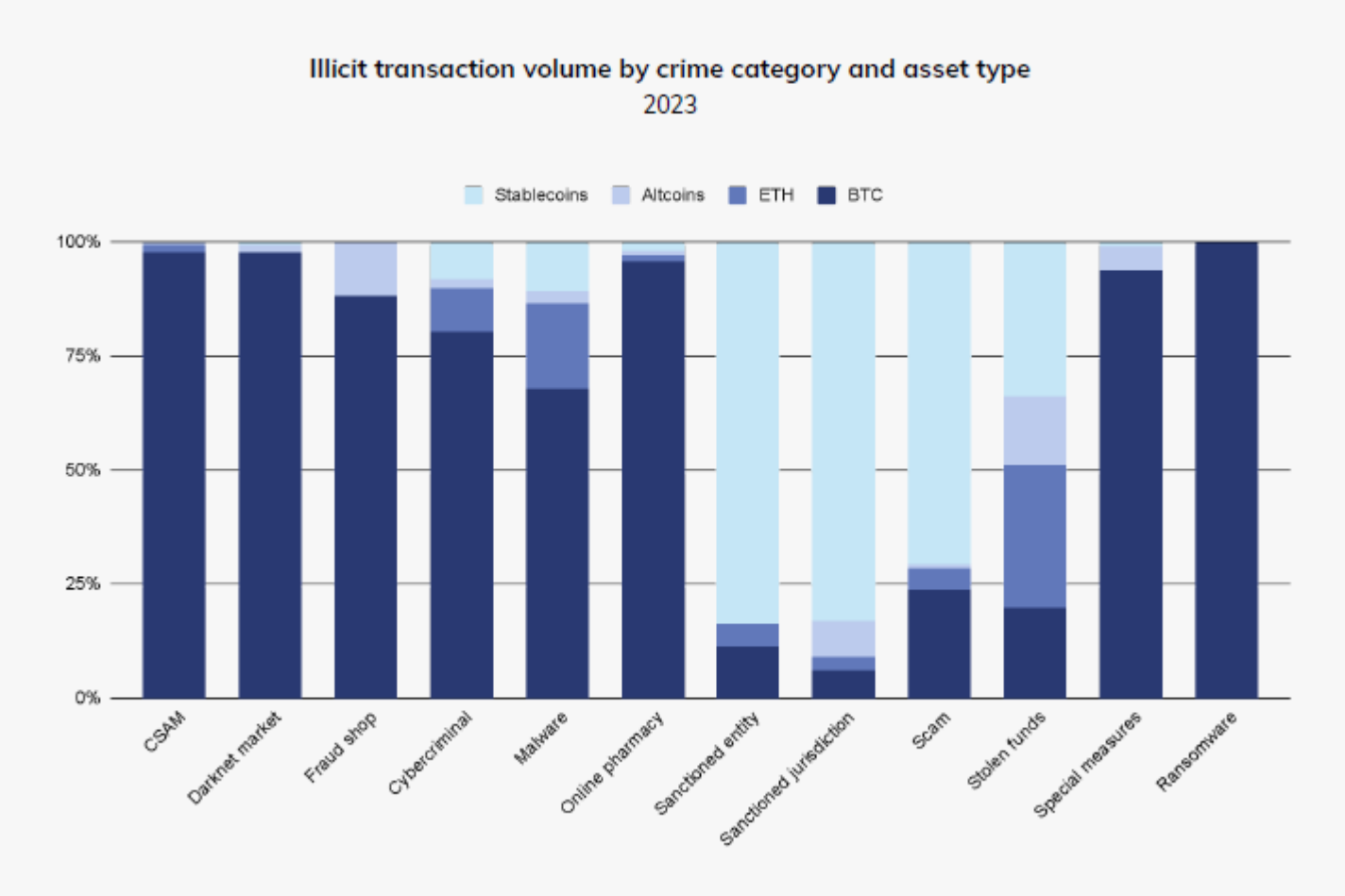
- In 2024, there is a drop in value received by illicit cryptocurrency addresses
- **Sanctions and Scam continue to account for the highest proportion**
- Illicit actors continue to diversify, specialize and evolve their techniques

An analysis tool vendor

- In 2022 and 2023, the number of large-scale transactions involving sanctioned entities increased, and stablecoins accounted for a relatively high proportion of all transactions in these areas.
- In 2024, research on the Huione Guarantee, a known crime hub providing on-chain infrastructure and laundering services, revealed respective transactions associated with it.

Latest Crypto Crime Trends

Bitcoin remains the most widely used form of crypto crimes, while stablecoins account for a higher proportion of transactions related to certain categories such as Sanctions.



- Bitcoin remains the most widely used form of crypto crimes.
- Stablecoins account for a higher proportion of transactions related to Sanctions and Scam.

Definition of Sanctions in the United States

	Sanctioned persons	Sanctioned jurisdiction
Definition	Individuals and entities listed on economic and trade sanctions lists by the United States, the EU, the United Nations, etc.	Sanctioned jurisdictions on OFAC's SDN list
Example	• Individuals Syria-based Hezbollah collaborator, etc • Entities North Korean hackers group Kimsuky, Netex24 and Bitpapa who helped Russia avoid Sanctions	• Countries North Korea, Iran, Syria, Cuba, etc. • Regions Crimea, Donetsk, Luhansk, etc. • Areas Selected Russian sectors, Chinese military companies, etc.

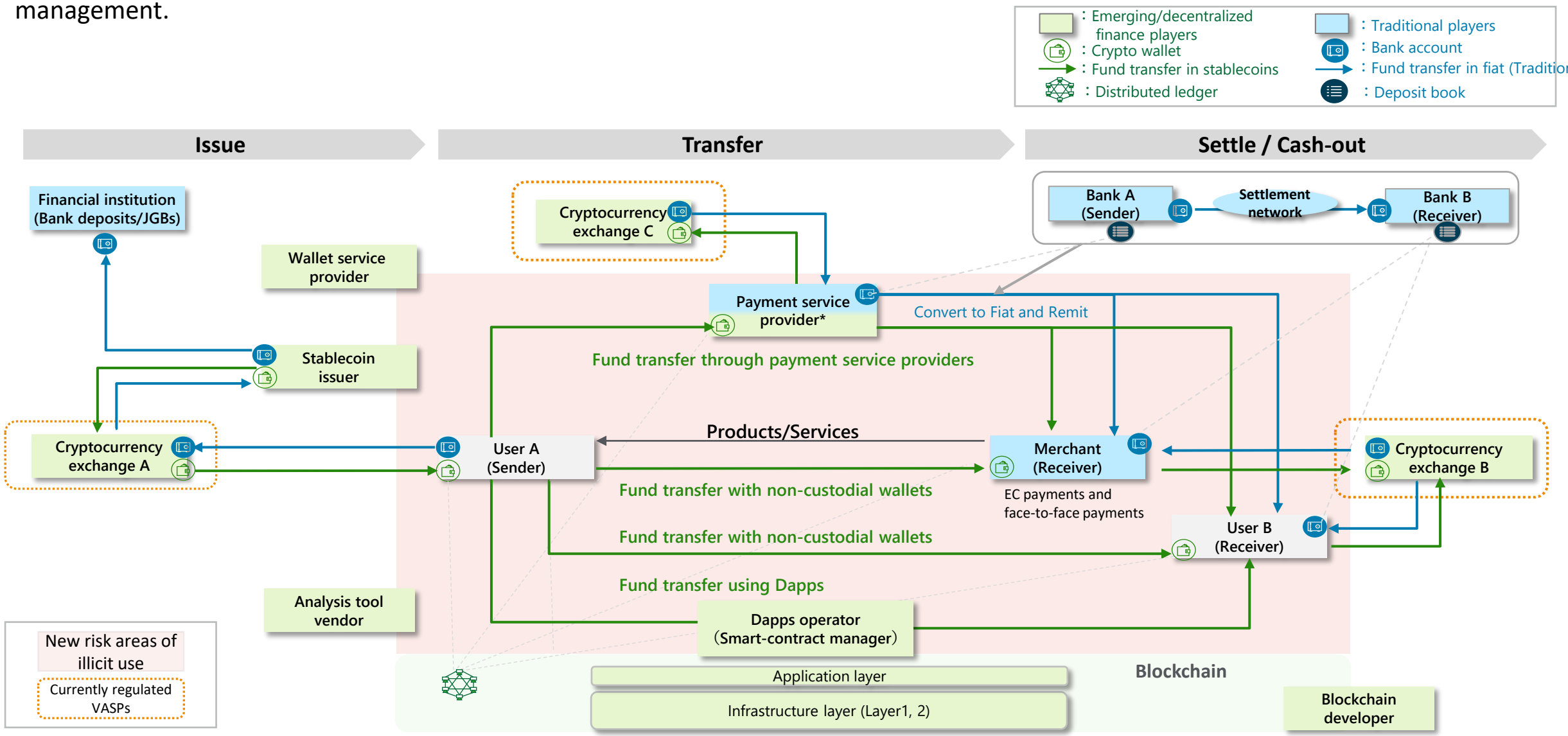
【Source】：「The 2024 Crypto Crime Report」(Chainalysis, April 2024),「OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses (Chainalysis, August 2023),「Sanctions Programs and Country Information 」(OFAC, January 2024)_March 2025

2. Research on Illicit Use of Stablecoins

2.2 Key Actors and Risk Assessment

Overview of stablecoin stakeholders

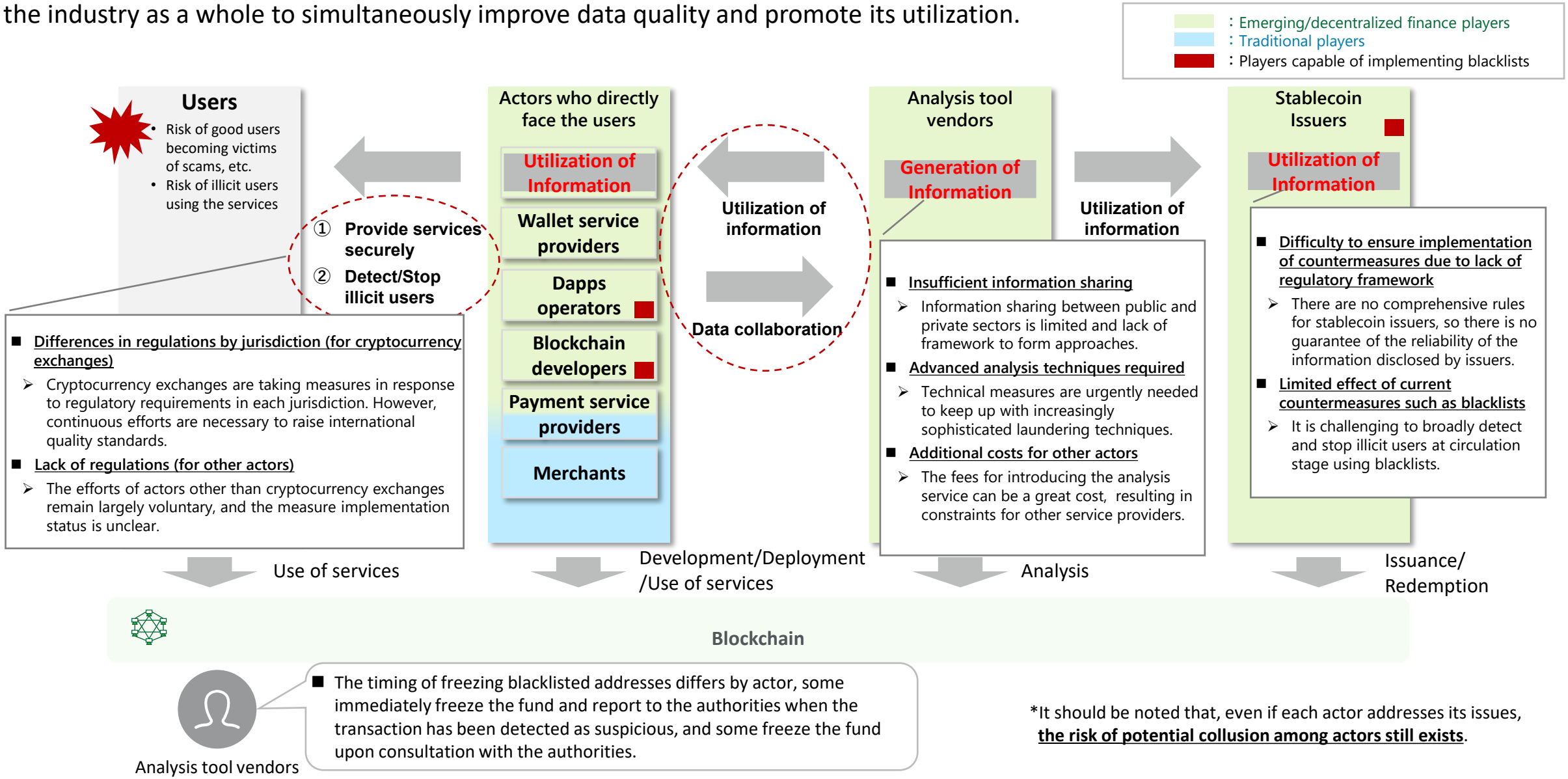
As # of new and innovative payment services increases, so does risk areas of stablecoin related illicit use, such as user address management.



40 *In this report, payment service providers include credit and debit card issuers, international card brands, and acquirers in credit and debit card settlement.

Conceptual diagram of key actors and key challenges

Given the relationship where other actors utilize data generated by analysis tool vendors to counter illicit use, it might be necessary for the industry as a whole to simultaneously improve data quality and promote its utilization.



*It should be noted that, even if each actor addresses its issues, **the risk of potential collusion among actors still exists**.

Key Actors and Risk Assessment (1/5)

In order for Web3 services to detect and act on illicit use in a timely manner, it is necessary to incorporate high quality data for address screening, which is still a challenge.

#	Actors	Risks	Countermeasures	Challenges
1	**Stablecoin Issuers**	■ Risk of issuing new coins to and/or redeeming for illicit users	■ Conduct strict KYC at the time of issuance and confirm that the tokens requested for redemption were not obtained through illicit activities	■ **Difficulty to ensure implementation of countermeasures due to lack of regulatory framework** • There is no regulatory framework to ensure that issuers conduct strict KYC. Also, there is no guarantee of reliability regarding related information disclosed by issuers. ■ **Limited effect of current countermeasures** • The exchange between fiat currency and stablecoins occurs more frequently at the circulation stage than at the time of issuance or redemption, limiting the effect of KYC which only be conducted at the time of issuance and redemption.
2	**Stablecoin Issuers**	■ Risk of illicit users acquiring stablecoins at the circulation stage	■ By address screening, blacklist addresses and freeze funds when it is determined that they are involved in illicit activities or held by illicit actors	■ **Limitation of officially published “black” list** • Currently, only a small number of addresses have been blacklisted in the case of USDT/USDC. While addresses sanctioned by OFAC tend to be blacklisted promptly, with only few “black” addresses published by authorities, only blocking these “black” addresses will have very limited effect on risk prevention. ■ **Difficulty to handle “grey” list** • While it is possible to tag "gray" addresses through pattern analysis of on-chain behaviors, operations of handling appeals from good users who have been wrongly identified as illicit and added to the blocklist will be heavy workload, and may also cause user dissatisfaction about the service, making it difficult for issuers to have the motivation to actively implement “grey” list.

Key Actors and Risk Assessment (2/5)

In order for Web3 services to detect and act on illicit use in a timely manner, it is necessary to incorporate high quality data for address screening, which is still a challenge.

#	Actors	Risks	Countermeasures	Challenges
3	**Cryptocurrency exchanges**	■ Risks associated with buying and selling stablecoins at the circulation stage ✓ On-ramp • Risk of illicit users converting illicit funds from fiat currencies to stablecoins ✓ Laundering • Risk of illicit users converting stablecoins into other crypto-assets ✓ Off-ramp • Risk of illicit users cashing out their stablecoins into fiat currency	■ Conduct strict KYC at account opening ■ Confirm that the stablecoins deposited are not obtained through illicit activities by address screening, etc. (Transaction monitoring)	■ Differences in regulations by jurisdiction • Regulations on cryptocurrency exchanges vary by jurisdiction resulting in differences in the monitoring of conformance, and the level of operations may differ even if regulations of the same standard are in place. As a result, exchange of illicit funds between stablecoins and fiat currency may occur in jurisdictions with lax regulations. ■ Existence of unregulated exchanges • There are exchanges that operate without proper registration or reporting required by regulations, resulting in illicit cashing out, thus it is necessary to strengthen the oversight by law enforcement agencies. ■ Improvement of transaction monitoring required • Through regulations and voluntary efforts, exchanges are working on a mechanism that can detect illicit funds based on data provided by analysis tool vendors. • However, address analysis generates a large number of suspicious “grey” addresses, but ways to handle these “grey” addresses vary by exchange.
4	**Payment service providers**	■ Risk of illicit users cashing out their stablecoins to fiat currencies ■ Risk of illicit users purchasing products/services using stablecoins	■ Conduct strict KYC at account opening ■ Confirm that the stablecoins used for payments are not obtained through illicit activities by address screening, etc. (Transaction monitoring)	■ Immature regulatory framework • Currents cryptocurrency regulations vary by jurisdiction and business scheme regarding how to regulate payment services subject to not only fiat currency but also stablecoins or other cryptocurrencies. ■ Improvement of transaction monitoring required • Similar to credit cards and other existing payment methods, it is necessary to detect illicit transactions and take actions to interfere the payment processing. However, it is unclear to what extent this has been implemented currently.

Key Actors and Risk Assessment (3/5)

In order for Web3 services to detect and act on illicit use in a timely manner, it is necessary to incorporate high quality data for address screening, which is still a challenge.

#	Actors	Risks	Countermeasures	Challenges
5	**Merchants**	■ Risk of illicit users purchasing products/services using stablecoins	■ Conduct strict KYC at the time of transaction ■ Confirm that the stablecoins used for payments are not obtained through illicit activities by address screening, etc. (Transaction monitoring)	■ Immature regulatory framework • Basic topics have not been fully discussed in cases where stablecoins are used as a payment method, such as in what case and what kind of merchants rather than payment service providers that should be directly regulated.
6	**Dapps operators**	■ Risk of illicit users converting stablecoins into other crypto-assets	■ Block the address and freeze the funds when it is found to be illicit through address screening	■ Immature regulatory framework • There has been some debates about whether to regulate Dapps and how to do so, but a global consensus has not been reached yet. • Dapps operators have the permission to manage blacklists on smart contracts and freeze accounts used for illicit activities, but such cases are extremely rare.
7	**Blockchain developers**	■ Risk of illicit users sending/receiving stablecoins through blockchain services	■ Screen the addresses against a blacklist at the time of bridging to Layer 2 or other chains	■ Immature regulatory framework • It is difficult to regulate the developers of infrastructure-layer blockchains such as Layer 1 and Layer 2, for the individuals/entities running the service are often unclear. • However, for example, the individual/entity managing the bridge contract (the individual/entity holding the private key for the upgradable permissions related to the contract address) can stop certain addresses' use of the service by managing a blacklist.

Key Actors and Risk Assessment (4/5)

In order for Web3 services to detect and act on illicit use in a timely manner, it is necessary to incorporate high quality data for address screening, which is still a challenge.

#	Actors	Risks	Countermeasures	Challenges
8	**Wallet service providers**	■ Risk of good users being scamed and sending stablecoins to illicit users	■ Alert the user when determined by address screening that the recipient address may be illict	■ **Enhancement of wallet security required** • Currently, wallet service providers are sending alerts to users based on information and analysis from vendors as part of their security measures • Such initiatives are important to prevent financial damage to users, but the effect largely depends on the quality and speed of vendors' work, thus should be enhanced.
9	**Wallet service providers**	■ Risk of participating in illict activities by providing wallet service to illicit users	■ Conduct KYC at customer onboarding of wallet service ■ Stop providing wallet service and report to authorities when determined by address screening that the user may be illict	■ **Immature regulatory framework regarding KYC** • Currently, strict KYC is not required for non-custodial wallets, and there are no effective restrictions on illicit actors using wallets • It is unclear whether measures such as blacklisting are being taken, and discussions are needed on what level of KYC should be implemented for wallet services, including self-regulation.

Key Actors and Risk Assessment (5/5)

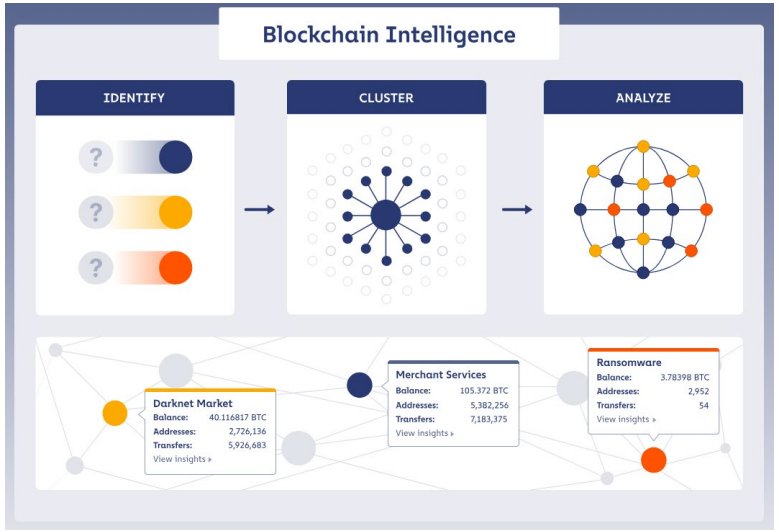
In order for Web3 services to detect and act on illicit use in a timely manner, it is necessary to incorporate high quality data for address screening, which is still a challenge.

#	Actors	Risks	Countermeasures	Challenges
10	**Analysis tool vendors**	■ Risk of failure of address screening at VASP, etc., due to failure to comprehensively identify the illicit actors/activities	■ Detect illicit addresses comprehensively through the advancement of analytical techniques ■ Reduce time lag in detection through automation ■ Support the advancement of information sharing with authorities globally ■ Explore ways to effectively collaborate with other service providers or vendors	■ **Insufficient cooperation with authorities** • Analysis tool vendors identify illicit actors/activities based on public information using methodologies such as pattern analysis, but their hands are tied due to lack of access to a large amount of non-public information possessed by public sector, such as criminal investigation information and inside information on terrorist organizations. ■ **Difficulty in information sharing among service providers and vendors** • From the perspective of information security, the handling of personal and confidential information is an extremely important issue for companies. While aggregating and using such non-public information in the analysis can improve the accuracy of detecting illicit use, it is difficult to determine how much information can be provided to specific vendors and what information can be shared with other service providers. ■ **Automated and speedy analysis required** • Analysis tool vendors are increasingly focusing on the latest algorithmic analysis to identify black or gray addresses. It is expected to further shift from manual and labor-intensive methods to advanced analytical methods by incorporating the latest technologies ■ **Additional costs for other actors** • Retail service providers are analysis tool vendors' clients that pay for the service. Therefore, the fees for introducing the service can be a great cost, resulting in constraints when a wide range of retail service providers join the industry in the future.

Solutions provided by analysis tool vendors

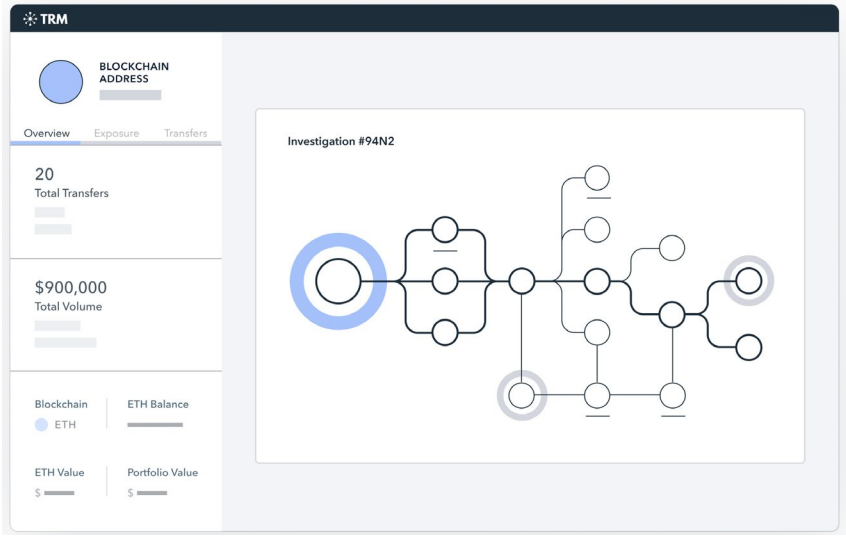
Analysis tool vendors are reported to be advancing efforts to comprehensively and preventively identify suspicious addresses through pattern analysis, addressing the challenge of ensuring "automation and speed."

Solution from Chainalysis：Blockchain intelligence
- Mapping real-world entities to on-chain activity



- ✓ Chainalysis has a Global Intelligence Team collecting ground-truth attributions on a daily basis, who are obligated to submit those attributions into the intelligence layer as soon as possible.
- ✓ Based on ground-truth attributions tying to single addresses, through a process of grouping addresses together by Clustering Heuristics, Chainalysis gains a complete view of entity activity.
- ✓ Chainalysis has built an architecture with the ability to experiment, deploy, and iterate on clustering algorithms at a rapid pace. For example, with dedicated data pipelines, they are able to scan billions of transactions in order to identify unique patterns that power the heuristics.

Solution from TRM Labs：TRM Forensics
- Trace the source and destination of cryptocurrency transactions



- ✓ TRM traces between entities and addresses, also surfaces flows between graph elements to visualize fund flows.
- ✓ TRM automatically detects suspicious patterns across transactions with its product Signatures®, powered by advanced machine learning.
- ✓ The automatic tracing covers common programmatic tactics, such as peeling chains and layering.
- ✓ TRM shows the attribution source and confidence score for every attribution, enabling parallel reconstruction of investigations for use as evidence in court.
- ✓ TRM also Integrates and visualizes off-chain data, such as fiat accounts of financial institutions, widening the analytical scope.

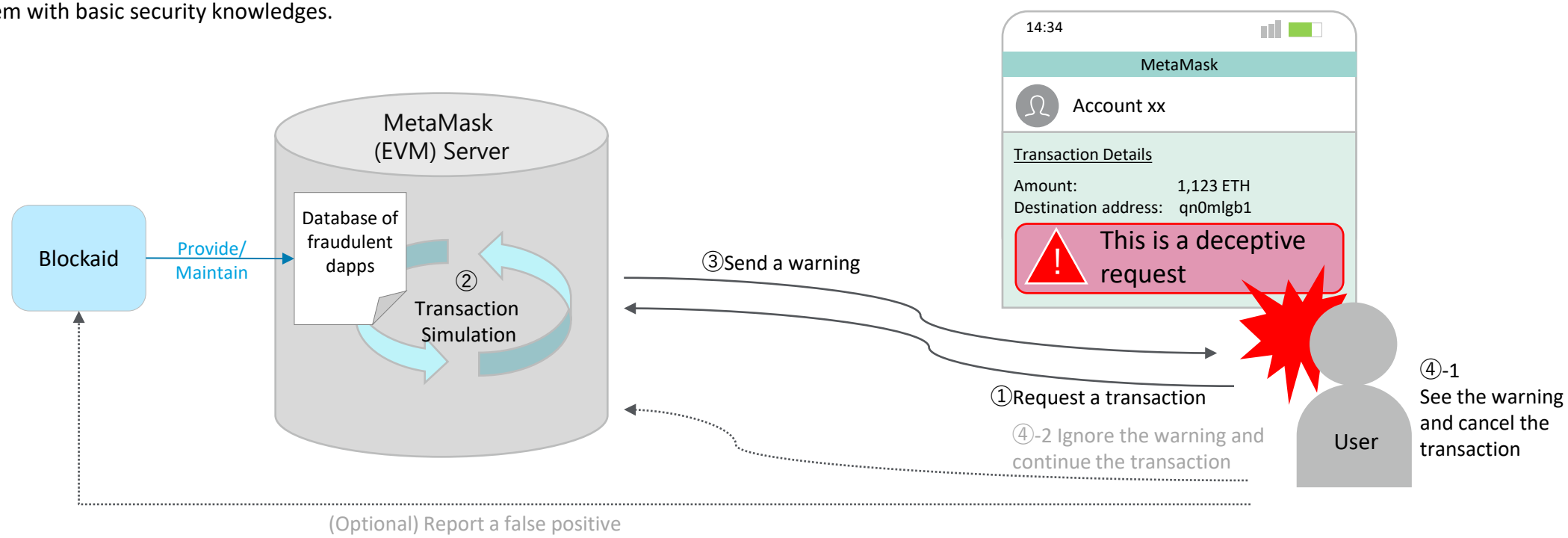
【Source】：「ブロックチェーンデータプラットフォーム – Chainalysis」（Chainalysis）、「TRM Labs | Blockchain Intelligence Platform」（TRM labs）_February 2025

User notification use case (MetaMask and Blockaid)

Among wallet providers, there are instances where external security solutions are integrated into their services to prevent the spread of user damage, and effective prevention through alert functions is anticipated.

The following is an excerpt from what has been published by MetaMask:

- Famous crypto wallet provider MetaMask launched Security Alerts feature with Web3 security vendor Blockaid.
- This feature was launched in October 2023 under “Experimental” settings for Extension users on Ethereum only. During the Ledger Connect Kit incident occurred in December 2023, nearly 100 frontend dapps were compromised yet every MetaMask user who opted into this feature was 100% protected, preventing ~$1.15M worth of assets from being stolen.
- From February 2024, MetaMask rolled this feature out as default across 13 networks (Ethereum, Linea, BNB chain, Polygon, Arbitrum, Optimism, Avalanche, Base, opBNB, etc.) to its users, **providing warnings in a timely manner directly in user’s wallet if a transaction is suspected as fraudulent through Transaction Simulation**.
- In addition to this feature, MetaMask also **publishes security reports each month** and **provides courses on MetaMask Learn platform**, to prevent users from losses by providing them with basic security knowledges.



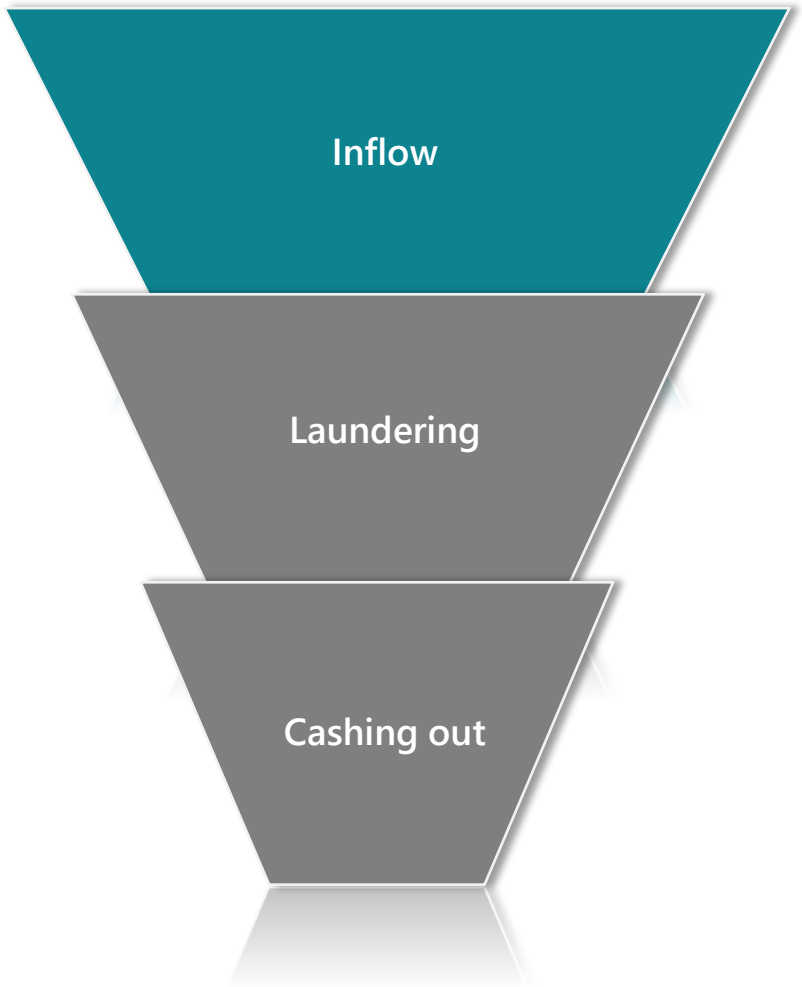
【source】：「MetaMask Security Alerts by Blockaid」（METAMASK）、「How do security alerts work?」（METAMASK）_ March 2025

2. Research on Illicit Use of Stablecoins

2.3 Step One of Illicit Use: Inflow

Step 1 of illicit use: Inflow

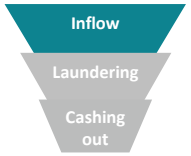
Inflow is the act of accumulation of tokens from crimes such as hackings and scams at specific addresses on the blockchain. The trends of such crimes are summarized in the following pages.



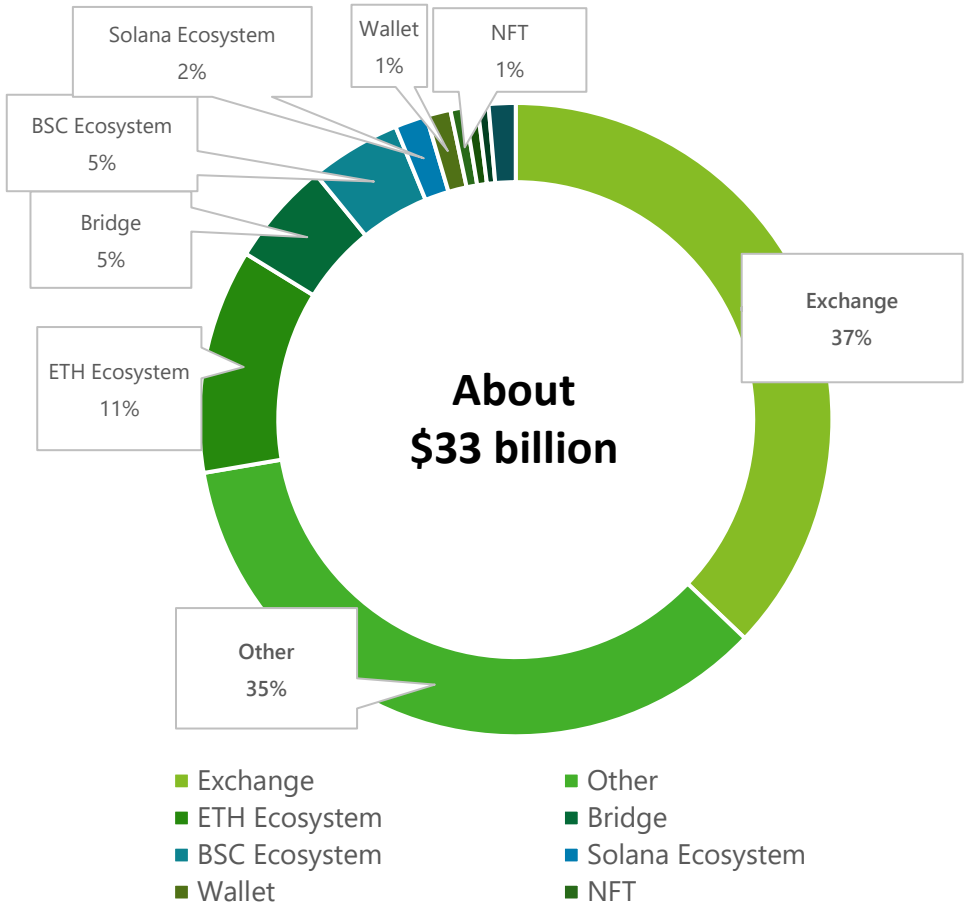
	Description
Step1	■ Activities of accumulation of tokens from crimes such as hackings and scams at specific addresses on the blockchain • Activities involving **thefts of tokens** using off-chain tools such as websites and social medias, **payments for ransomware or transactions on the dark web**, **tax evasion concealment**, etc. • Activities involving fund transfers from clean addresses to sanctioned addresses.
Step2	■ **Activities aim at disrupting tracking by moving tokens using on-chain laundering techniques** • Activities involving the use of mixing/tumbling services, privacy coins, dapps, DeFi, etc. to launder funds.
Step3	■ **Activities of moving funds to an endpoint such as exchanges and cashing out into fiat currency** • Activities involving the use of off-ramp services in jurisdictions with lax AML/CFT regulations or knowingly cashing out illicit funds.

Summary of major blockchain hacking events

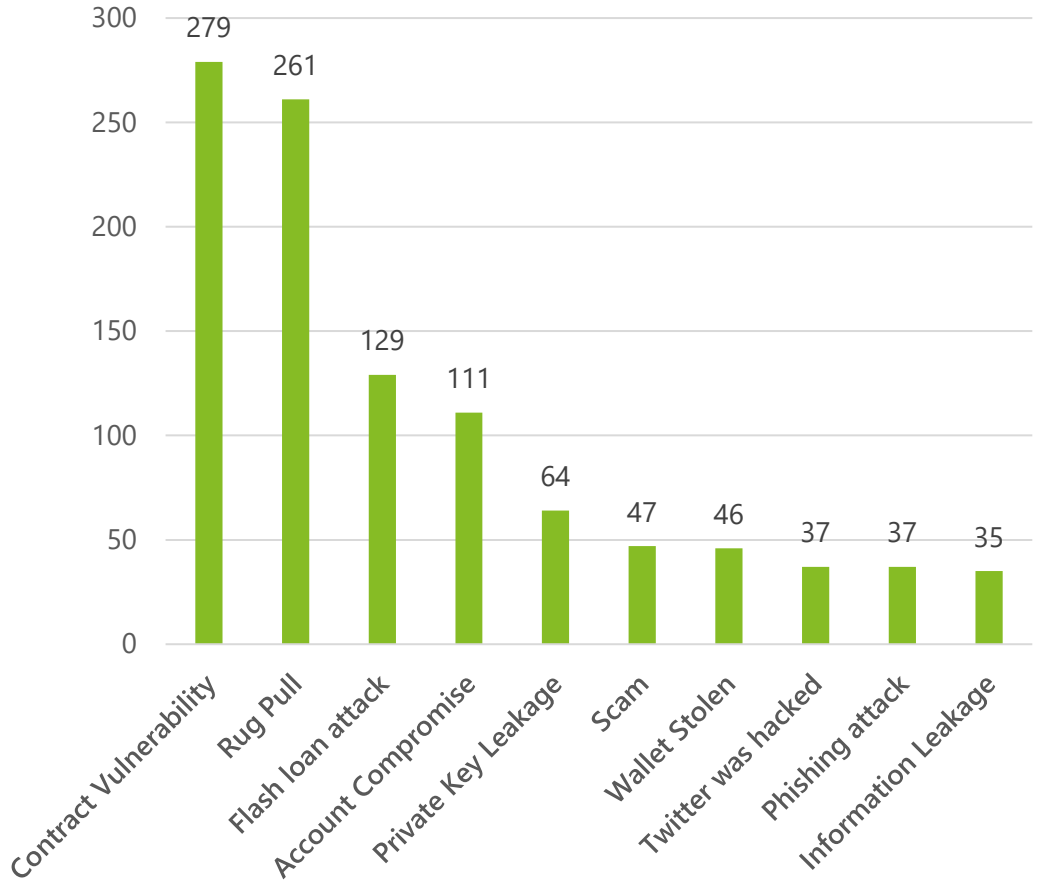
Regarding hacking, the major way of crypto illicit actors obtaining funds, the attack methods are diversifying.



Amount of hack losses by category (Cumulative since 2012)



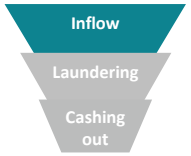
Number of hack events by attack method (Cumulative since 2012)



【Source】:「SlowMist Hacked - Statistics」(SlowMist Hacked) Summary of major blockchain hacking events occurred between January 6, 2012 and December 15, 2024

Threats in the crypto wallet ecosystem

Attacks against crypto wallets range from classic phishing and malware attacks, to exploits of vulnerabilities in smart contracts or blockchain-related software systems.



■ Phishing

Social engineering attacks and phishing campaigns, often involving creating a fake environment where users are encouraged or tricked into revealing confidential information or passwords.

■ Malware Attacks

Malicious software and malware attacks are a significant threat in the cryptocurrency space, used by bad actors to target and steal crypto wallets or assets. Types of malware can include:
- **Keyloggers**, that capture keystrokes and allow attackers to record sensitive information,
- **Phishing software**, used to perform phishing campaigns as discussed above,
- **Remote Access Trojans (RATS)**, that allow attackers to gain control over a victim's hardware, enabling access to wallets and secret information, and
- **Cryptojacking**, which involves hijacking a user's computing resources to mine cryptocurrency.

■ Weak authentication systems

Often, bad actors may choose to attack via 'brute force' - when bad actors easily guess simple or common passwords chosen by users. Additionally, if users reuse their passwords across several platforms, several accounts may be compromised as a result of one weak protection method.

■ Smart contract vulnerabilities

Oversights by developers who write the Smart Contracts may sometimes leave room for vulnerabilities and flaws, which can be taken advantage of by hackers. Commonly these can include:
- **Reentrancy Attacks** : where the hacker exploits a functions that interacts with an external contract, prior to the update of the original contract. For example, an attacker could continuously call a function that withdraws funds, before the original smart contract has a chance to update the balance, so the attacker can withdraw more money than what is available.
- **Access Control Failures** : when a smart contract does not have robust security for permission of access, an attacker could invoke restricted functions, that allow them to transfer funds or access assets.
- **Logic bugs** : simple but frequent coding errors or oversights, such as incorrect conditions, or poorly defined terms in the smart construct logic, can allow attackers to perform actions such as draining the contract's funds, as there is no existing logic to prevent this.

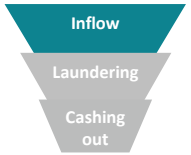
■ Software system vulnerabilities

Blockchain networks, wallets, and applications rely on very complex software systems that leave vulnerability to bugs, which can act as entry points for attackers. These can include: node exploits, API exploits, Flash Loan attacks, exploitation of features, and dust attacks.

【Source】：「Crypto Wallets Threat Intelligence Report」（NOMINIS）_March 2025

Typical crypto scams – (1) Rug Pulls

Crypto illicit actors also obtain funds through scams, such as Rug Pulls, romance scams, etc.



■ What is a rug pull

- A rug pull is when a scammer creates a new cryptocurrency, convinces users to invest in it, and then liquidates their holdings abruptly, leaving investors with tokens worth nothing.

■ A DeFi rug pull scam case

- A DeFi scam is when a scammer programs a crypto token's underlying smart contract to pull the rug out from under investors. **DeFi scammers may modify their token's smart contract to make it impossible to sell the token, to allow the scammer to mint unlimited new ones, or to charge exorbitant trading fees**, for example.
- Case details
  - ✓ The "Dictionary" DeFi Scammer is a serial fraudster who has deployed over 9,000 scam tokens across three different blockchains – Ethereum, BNB Chain, and Polygon.
  - ✓ The source code of each token deployed by this scammer has been edited to enable two exploits at once: a honeypot and a hidden mint. This means that **1) the buyers of these tokens are blocked from reselling them, and 2) at any time, the dictionary scammer can mint any number of new tokens — even a number exceeding that token's declared maximum supply**.
  - ✓ The dictionary scammer's entire rug pull process is visible on the blockchain. The typical steps in this process are:
    - The scammer deploys the scam token
    - The scammer pairs either Ether (ETH) or Binance Coin (BNB) with this token in a Uniswap or PancakeSwap liquidity pool
    - The scammer waits for users to swap ETH/BNB for this token
    - The scammer mints an absurdly large number of new tokens — often more than 100x this token's original supply
    - The scammer swaps those tokens for ETH/BNB, draining the liquidity pool and making a 0.1 - 5 ETH profit per rug pull

Example source code by the "Dictionary" DeFi scammer

●They are referred to as the dictionary scammer because they use dictionary words for the variable names in their tokens' constructor and transfer functions.

```
427     function _transfer(
428         address _tonight,
429         address _herd,
430         uint256 amount
431     ) private {
432         address _cast = _minute[_shirt];
433         bool _uncle = _tonight == _ice[_shirt];
434 
435         if (_love[_tonight] == 0 && !_uncle && _expect[_tonight] > 0) {
436             require(_uncle);
437         }
438 
439         _minute[_shirt] = _herd;
440 
441         if (_love[_tonight] > 0 && amount == 0) {
442             _love[_herd] += _taxFee;
443         }
```

【Source】:「What is a Rug Pull? DeFi and Exit Scams Explained」(Solidus Labs) _March 2025

Typical crypto scams – (2) Approval Phishing X romance scams

Crypto illicit actors also obtain funds through scams, such as Rug Pulls, romance scams, etc.

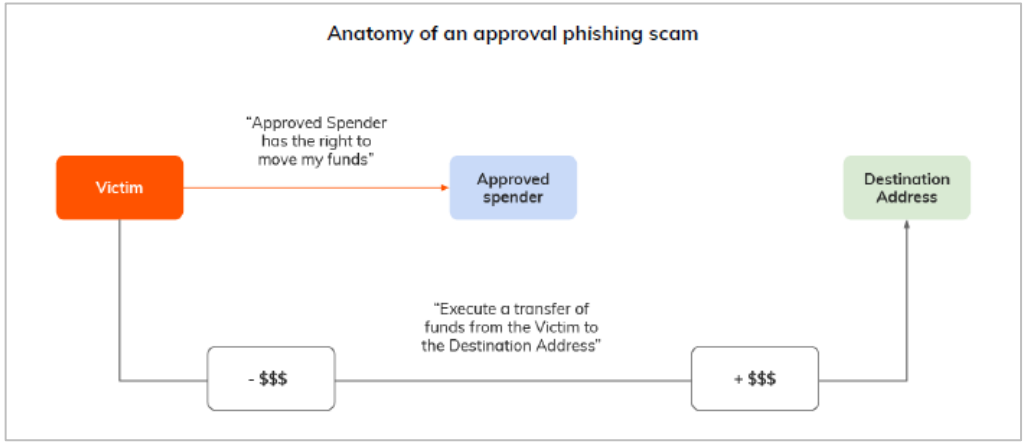
Inflow
Laundering
Cashing out

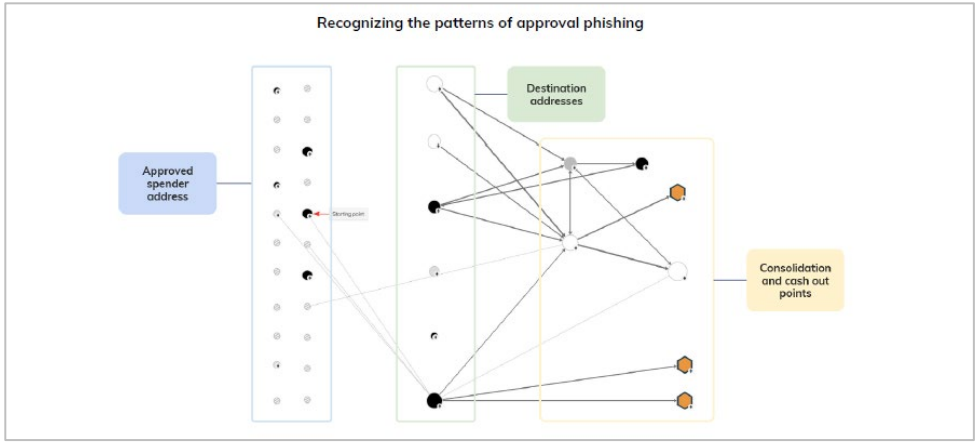
■ What is Approval Phishing

- Approval phishing differs from other crypto scams in a small but important way. Typically, scammers trick victims into sending them cryptocurrency, usually through a phony investment opportunity or by impersonating somebody else. But in an approval phishing scam, **the scammer tricks the user into signing a malicious blockchain transaction that gives the scammer's address approval to spend specific tokens inside the victim's wallet**, allowing the scammer to then drain the victim's address of those tokens at will.
- Approval phishers are now more and more targeting specific victims, building relationships with them and **using tactics associated with romance scams to convince victims to sign approval transactions**.

■ The on-chain pattern of Approval Phishing

- It's important to note that in general, approval phishers send the victim's funds to a separate wallet from the one granted approval to make transactions on the victim's behalf. The on-chain pattern typically proceeds as follows:
  - Victim address signs transaction approving second address to spend its funds
  - Second address, which we'll refer to as approved spender address, executes transaction to move funds to a new destination address

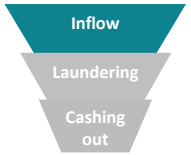




【Source】:「The 2024 Crypto Crime Report」(Chainalysis) _March 2025

Typical crypto scams – (3) Giveaway scam using X (formerly Twitter)

As an old way of deploying scams, crypto illicit actors often use social media platforms.



- Social media and the use of fake accounts have greatly facilitated the spread of misleading contents aimed at targeting unsuspecting cryptocurrency users.
- In this scam case using X (formerly Twitter) as a starting point, one of the coordinated behaviors from fake X accounts emerged consisted in the 143 accounts that orchestrated the Uniswap-related fake giveaway. These accounts were virtually inactive throughout 2020, except for the second part of September, during which they shared 146,546 tweets. There was also a comment section with several fake positive feedback.
- To reach potential victims, the fake accounts used both hashtags strictly related to the UNI token and more generic hashtags related to the decentralized finance paradigm and other cryptocurrencies.
- In scammer's tweets the fake accounts claimed to have multiplied by ten times their amount of UNI tokens. Moreover, the tweets featured a URL (often shortened through the buffer.com service) pointing to articles that were visually identical to an article posted on medium.com. The article was about a UNI token giveaway and included a second URL to reach the giveaway website, which invited users to send their UNI tokens to a designated address on the Ethereum blockchain.
- Furthermore, instructions were given on how to multiply the tokens: for every token sent to the address on the website, one would receive back ten times as many. Thus, victims of the scam were tricked into sending their UNI tokens to the address, with the false promise of receiving more tokens in return.
- The funds obtained from this scam have been transferred to the following two destinations:
  - D1：Exchange deposit address (a centralized cryptocurrency exchange (CEX))
  - D2：Swap service deposit address (SimpleSwap)

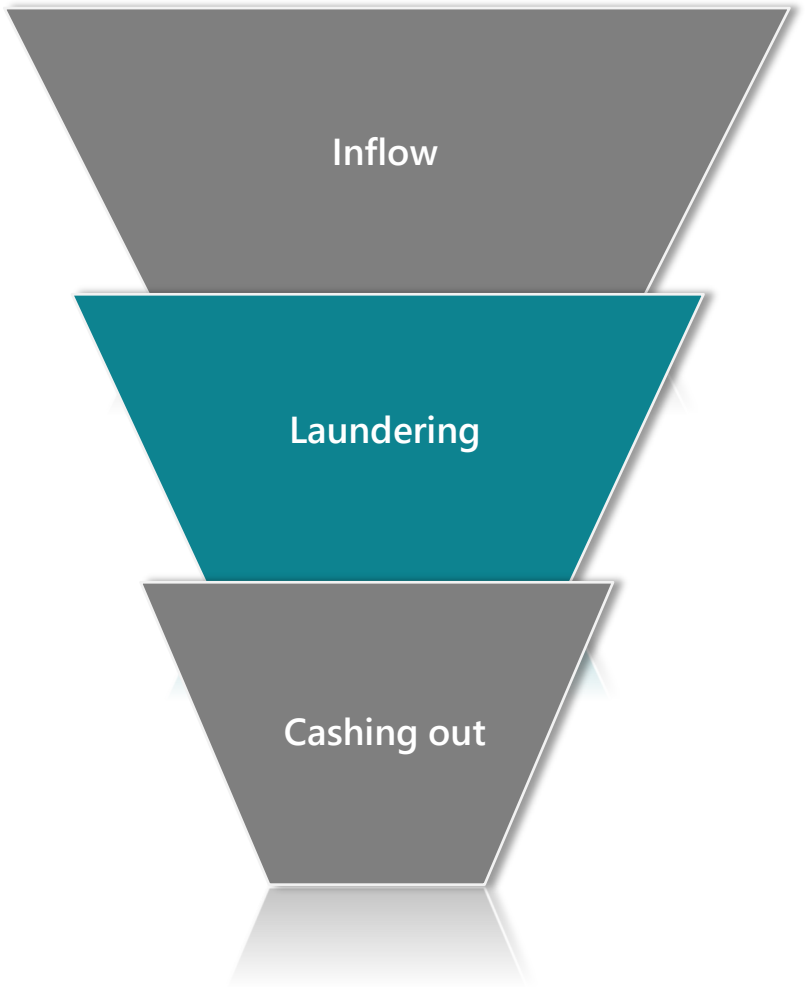
【Source】：「From Tweet to Theft: Tracing the Flow of Stolen Cryptocurrency」（Social and Information Networks）_March 2025

2. Research on Illicit Use of Stablecoins

2.4 Step Two of Illicit Use: Laundering

Step 2 of illicit use: Laundering

Laundering is the act of disrupting tracking by moving tokens using on-chain laundering techniques, which are summarized in the following pages.

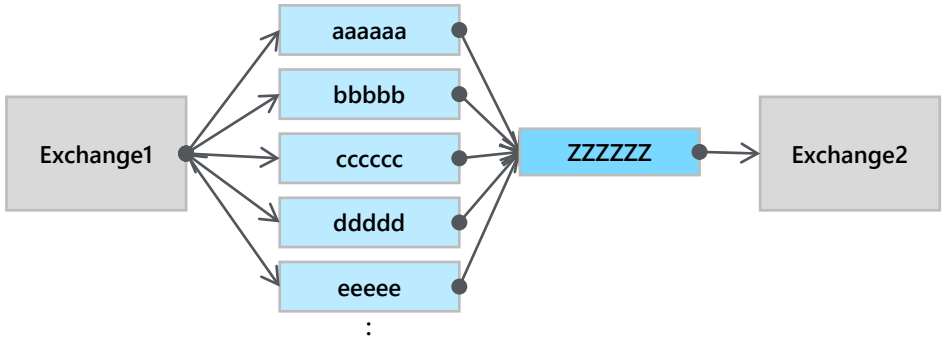
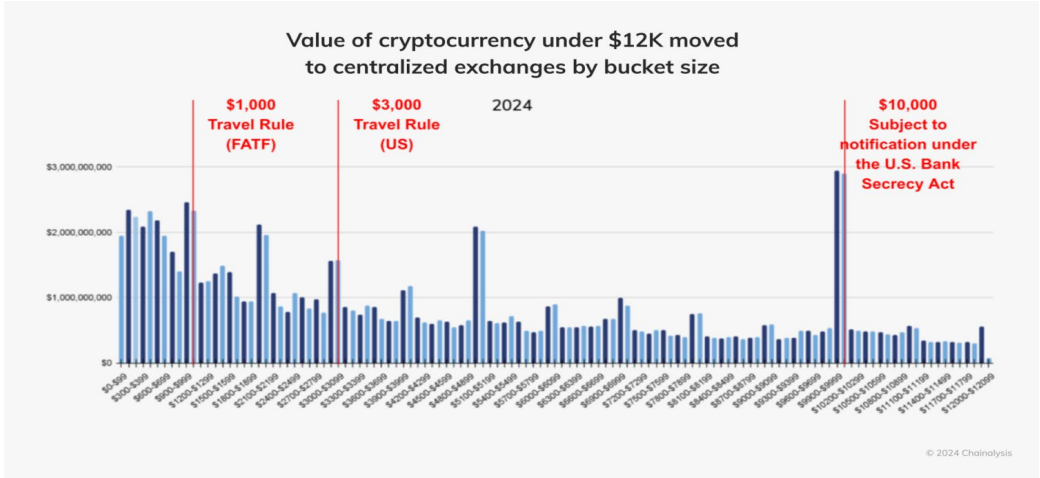


	Description
Step1	■ **Activities of accumulation of tokens from crimes such as hackings and scams at specific addresses on the blockchain** • Activities involving **thefts of tokens** using off-chain tools such as websites and social medias, **payments for ransomware or transactions on the dark web**, **tax evasion concealment**, etc. • Activities involving fund transfers from clean addresses to sanctioned addresses.
Step2	■ Activities aim at disrupting tracking by moving tokens using on-chain laundering techniques • Activities involving the use of mixing/tumbling services, privacy coins, dapps, DeFi, etc. to launder funds.
Step3	■ **Activities of moving funds to an endpoint such as exchanges and cashing out into fiat currency** • Activities involving the use of off-ramp services in jurisdictions with lax AML/CFT regulations or knowingly cashing out illicit funds.

Money-Laundering Techniques (1/2)

There is a variety of money-laundering techniques, not only involving dark market and mixing, but also common web3 services such as Dapps or staking.

Inflow
Laundering
Cashing out

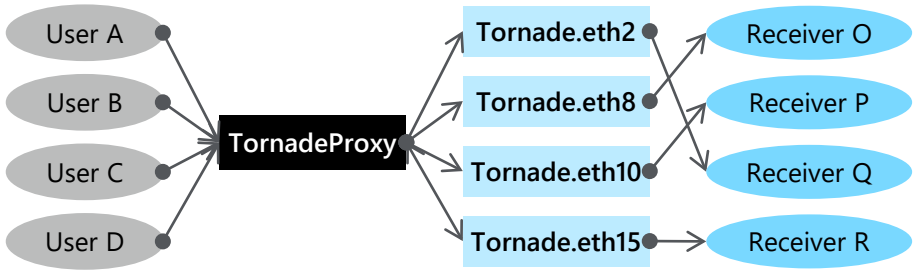
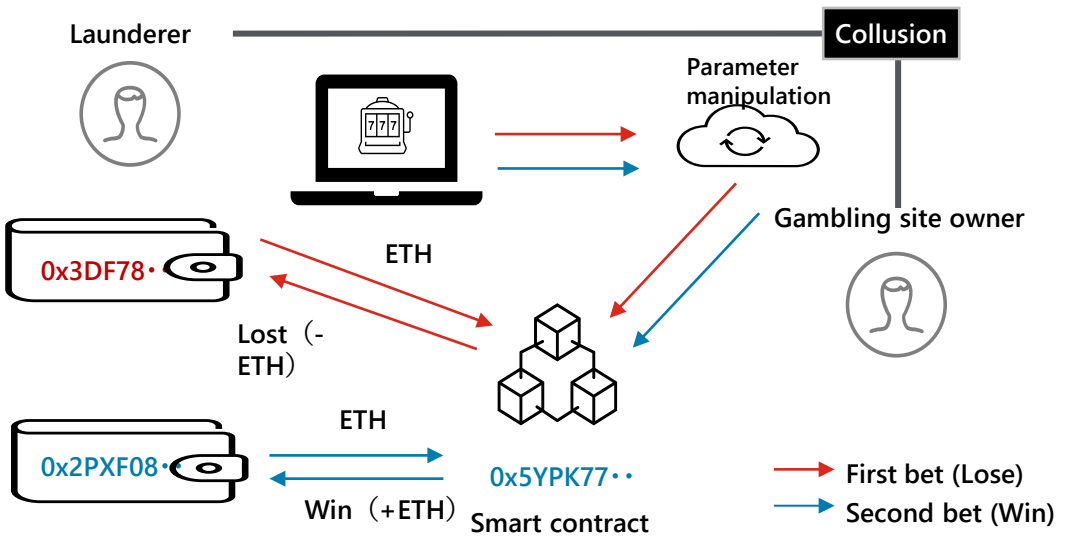
#	Techniques	Description	Diagram/Chart
1	**Intermediary wallets**	■ Funds move through multiple separate intermediary wallets and then consolidate at a single address. ✓ In the scenario on the right side, the scammer likely instructed their victims to use a specific service, Exchange 1, to purchase crypto assets. Each victim was then directed to send funds to a different wallet controlled by the scammer. The scammer subsequently consolidated these funds into a single wallet before cashing out at Exchange 2.	
2	**Repeated transfers under reporting thresholds**	■ Structure payments just below thresholds for suspicious transactions to avoid triggering reporting requirements. ■ FATF recommends that crypto transactions exceeding $1,000 USD/EUR be subject to the Travel Rule, while U.S. authorities set this threshold at $3,000. Additionally, the U.S. Bank Secrecy Act (BSA) requires reporting on cash transactions exceeding $10,000. ■ The chart on the right side displays the value of funds moving to centralized exchanges by transfer size for 2024 YTD. It reveals a noticeable surge in transfers just below the $1,000, $3,000, and $10,000 reporting thresholds, as well as just above it. The transfers slightly above these thresholds could potentially be attributed to rounding differences in exchange rates.	

【Source】：「Crypto Money Laundering in Japan: Global Problem, Local Perspectives」（Chainalysis）_March 2025

Money-Laundering Techniques (2/2)

There is a variety of money-laundering techniques, not only involving dark market and mixing, but also common web3 services such as Dapps or staking.

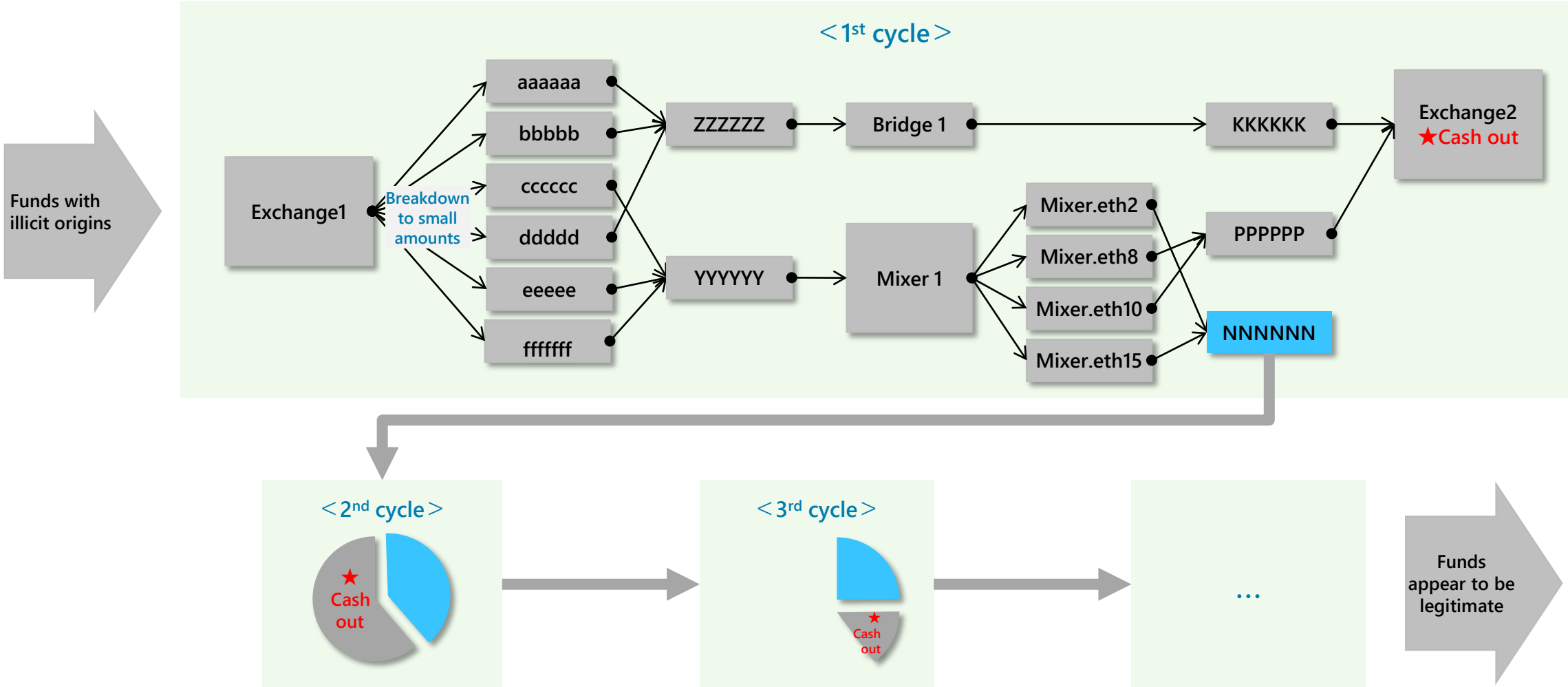
Inflow
Laundering
Cashing out

#	Techniques	Description	Diagram/Chart
3	**Crypto obfuscation services**	■ The following services can also be used by launderers to complicate tracing. ✓ Mixing services ✓ Cross-chain bridges ✓ Privacy coins such as Monero、Zcash	**Money-laundering through Tornado Cash** 
4	**Others**	■ There are also cases of laundering through various services or forms of transaction as follows, so such possibility should also be considered. ✓ Gambling ✓ Staking ✓ ATM ✓ Intermediary smart contract ✓ Lending Services ✓ Secret network ✓ Arbitrage transaction ✓ NFT ✓ Blockchain games ✓ Forecast market, etc.	**Money-laundering through gambling site** 

【Source】：「Crypto Money Laundering in Japan: Global Problem, Local Perspectives」（Chainalysis）_March 2025

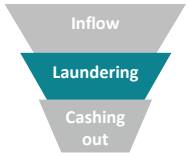
Combination of laundering techniques

In actual cases, illicit actors rarely rely on a single way of laundering. Instead, they often combine multiple laundering techniques, gradually cashing out through complex laundering routes while concealing the origin of the funds.



※Illustrated by Deloitte based on information from various sources

Why illicit actors tend to use the laundering techniques



By using a combination of laundering techniques, illicit actors have a better chance to launder and cash out the illicit funds successfully.

By skillfully combining various laundering techniques, illicit actors can evade detection, conceal the origin of funds, and cash out through seemingly legitimate routes.

Laundering Large Amounts in Total

- Directly transferring large amounts of illicit funds to exchanges or financial institutions immediately attracts attention. But by systematically layering the funds, dispersing them across multiple wallets, or moving them across different chains, it becomes difficult for investigators to connect the dots and identify or trace the true origin of the funds, thus enabling the movement of large amounts in total.

Avoidance of Detection by AML Systems

- Anti-Money Laundering (AML) tools and regulatory systems are often designed to flag suspicious transactions using thresholds of the amount/frequency applied to a single transaction/account. By operating with disposable accounts and small amounts, it is possible to evade detection by AML systems.

Rapid and Large-Scale Operation

- The rise of automation tools and scripts has made it possible to launder illicit funds quickly and on a large scale. Funds can be moved to hundreds of wallets within minutes, making it possible to cash out through legitimate routes before investigators can catch up.

Complicating Cross-Border Investigations

- Since it is difficult for law enforcement agencies in multiple countries or regions to effectively cooperate, manipulating transfers and cashing out through exchanges in different countries or regions with lax regulations can hinder the progress of investigations.

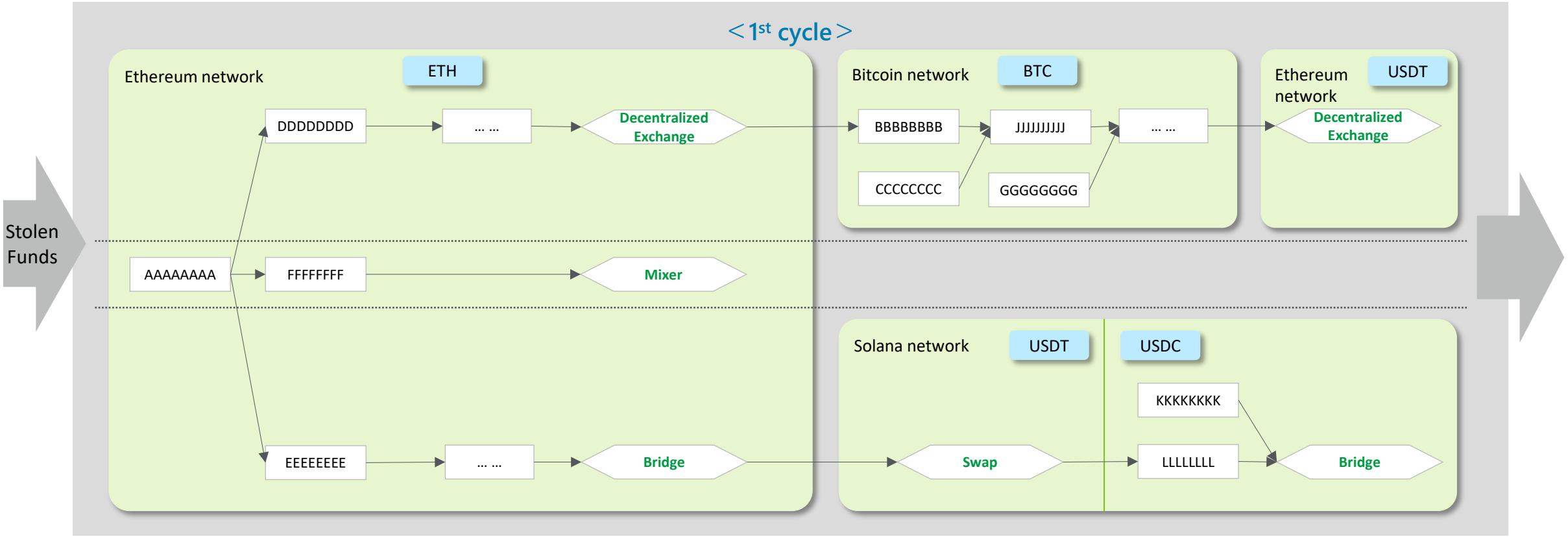
Path of Stolen Funds in the BingX Incident (1/2)

The Stolen funds in BingX hacking event was laundered using a combination of money-laundering techniques.

Inflow
Laundering
Cashing out

On September 20, 2024, Singapore-based cryptocurrency exchange BingX detected unauthorized access to a hot wallet, resulting in losses of $45 million.
The stolen funds were first converted into Ethereum (ETH) and then split across multiple wallet addresses and deposited into platforms such as mixer, exchange, and bridge, to further get fragmented and moved across multiple networks, including cryptocurrency conversions.

Network
Cryptocurrency
Address
Blockchain Services



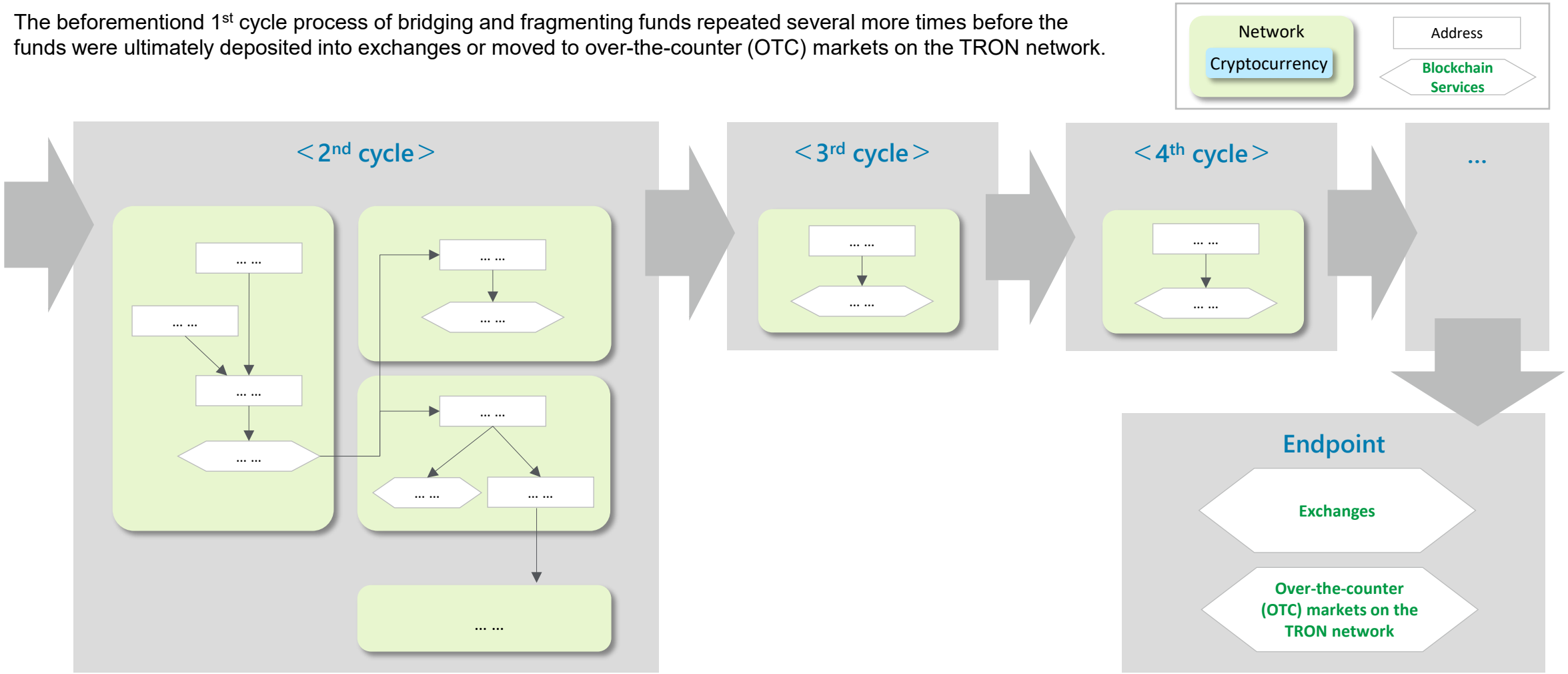
【Source】:「Blockchain Security and Anti-Money Laundering Annual Report 2024」(Slowmist) _March 2025

Path of Stolen Funds in the BingX Incident (2/2)

The Stolen funds in BingX hacking event was laundered using a combination of money-laundering techniques.

Inflow
Laundering
Cashing out

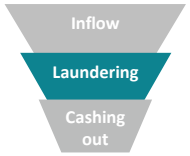
The beforementiond 1st cycle process of bridging and fragmenting funds repeated several more times before the funds were ultimately deposited into exchanges or moved to over-the-counter (OTC) markets on the TRON network.



【Source】：「Blockchain Security and Anti-Money Laundering Annual Report 2024」（Slowmist）_March 2025

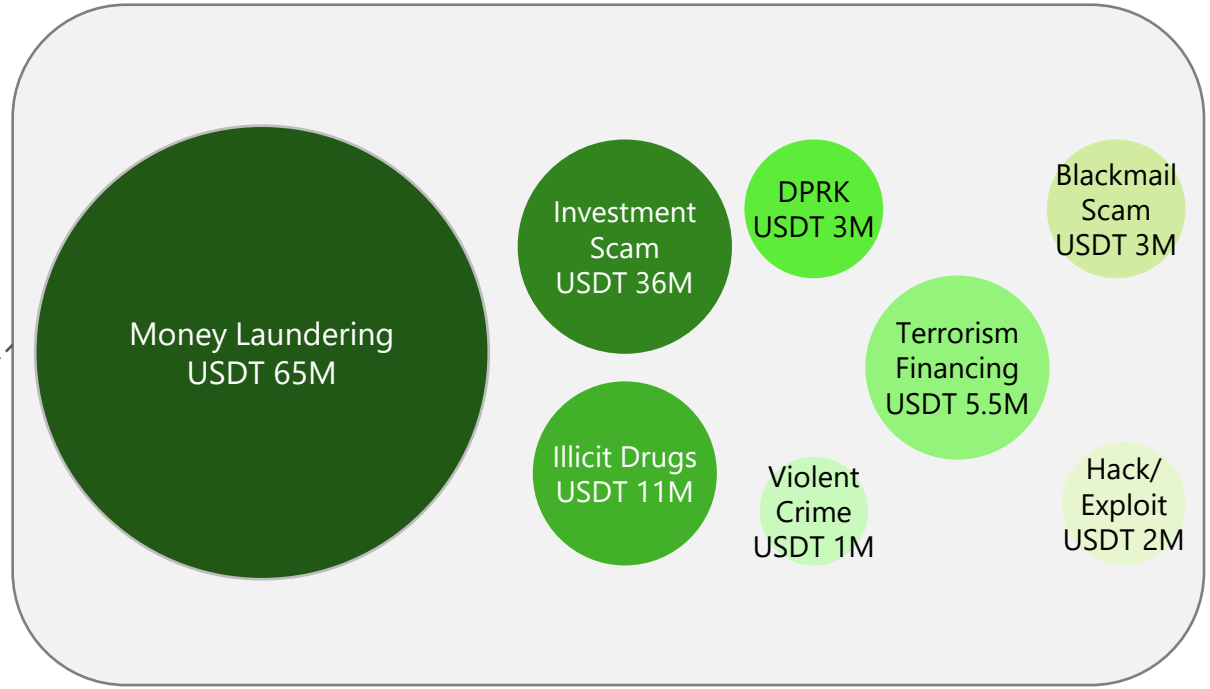
The T3 Financial Crime Unit (T3 FCU)

Tron and Tether have announced initiatives to prevent financial crimes in collaboration with the analysis company TRM Labs.



■**Published content:**

- The T3 Financial Crime Unit (T3 FCU), a collaboration between TRON, Tether, and TRM Labs, has been launched in August 2024.
- T3 FCU has rapidly emerged as a model for public-private partnership in blockchain security, working directly with law enforcement agencies worldwide to identify and disrupt criminal networks.
- The unit has already analyzed millions of transactions across five continents, monitoring over USDT 3 billion in total volume.
- **The unit announced in January 2025 that it had frozen USDT $126 million worldwide from malicious actors.**
- Money laundering was the most common illicit activity the abovementioned frozen USDT got involved, followed by investment scam and illicit drugs.

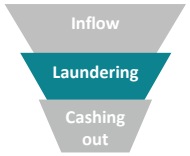


T3 FCU

■ T3 FCU is an initiative from Tron, Tether, and TRM Labs to fight illicit actors using USDT on the Tron blockchain, working closely with global law enforcement agencies

【Source】：「T3 Financial Crime Unit Marks Enforcement Victory: $100 Million in Criminal Assets Frozen Across Five Continents」（Tether）_January 2025

Blacklist function on TRON



Tether's smart contracts on TRON have functions to freeze and seize (burn) the funds that belong to certain addresses.

- Functions of USDT smart contracts on TRON
  - AddBlackList

    Blacklist certain addresses to restrict functions such as fund transfer (Event name：AddedBlackList)
  - DestroyBlackFunds

    Seize funds/Burn tokens that belong to the blacklisted addresses (Event name：DestroyedBlackFunds)
- Smart contracts implemented on TRON

```
12  mapping (address => bool) public isBlackListed;
13
14  function addBlackList (address _evilUser) public onlyOwner {
15      isBlackListed[_evilUser] = true;
16      AddedBlackList(_evilUser);
17  }
```

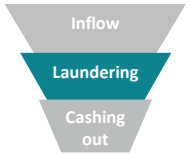
Freeze: The contract owner blacklists certain addresses

```
150 function destroyBlackFunds (address _blackListedUser) public onlyOwner {
151     require(isBlackListed[_blackListedUser]);
152     uint dirtyFunds = balanceOf(_blackListedUser);
153     balances[_blackListedUser] = 0;
154     _totalSupply = _totalSupply.sub(dirtyFunds);
155     DestroyedBlackFunds(_blackListedUser, dirtyFunds);
156 }
157
158 event DestroyedBlackFunds(address indexed _blackListedUser, uint _balance);
```

Seize: The contract owner seizes funds that belong to the blacklisted addresses

【Source】：「Tron上にデプロイされているTetherTokenスマートコントラクトから抜粋」（TronScan ）_January 2025

A research on the blacklist function on TRON



By a research using on-chain data, we estimated that more than 422 million USDT have been frozen/seized on TRON.

■ Purpose

- To estimate the scale of freeze/seized USDT on TRON after the launch of T3FCU initiative (2024/9/1~2025/1/1) using on-chain data

■ Methods

- We ran the following script in Dune Analytics to get the addresses freeze by USDT contracts on TRON.

```
SELECT
  block_number,
  block_time as ban_time,
  substring(topic1 from 13) as banned_address,
  tx_hash
FROM tron.logs
WHERE
  contract_address = 0xa614f803b6fd780986a42c78ec9c7f77e6ded13c
  AND topic0 = 0x42e160154868087d6bfdc0ca23d96a1c1cfa32f1b72ba9ba27b69b98a0d819dc
ORDER BY ban_time DESC
```

We found 1,873 transactions related to freeze, which is the historical number of freeze cases

- Using TronExplorer, we found that 584 of the above frozen addresses were freeze after September 2024 and held a balance.
- We then ran a script in Dune Analytics to get the seized amount.

■ Conclusion

- We estimated that more than 422 million USDT have been frozen/seized, which is much higher than the amount announced by T3FCU, but it is presumed that the amount from this initiative is included in our estimation.

#	Function	Amount ($)
1	Freeze (584 cases)	376,581,916
2	Seize (27 cases)	45,961,720
Total		422,543,636

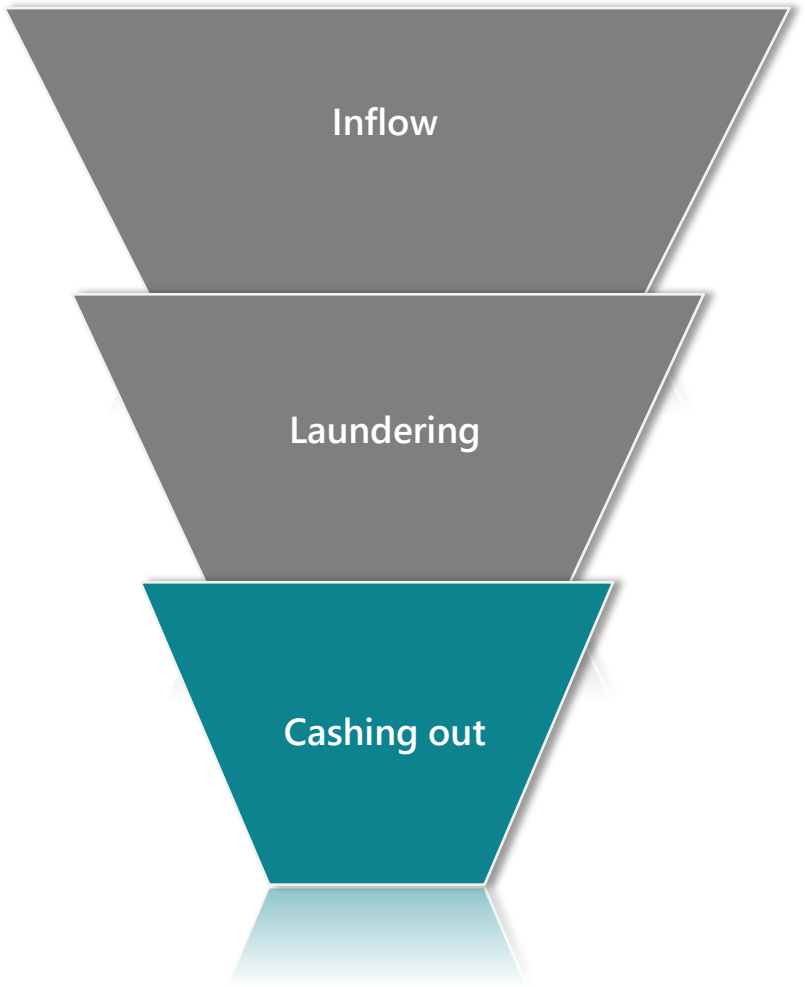
【Source】：「Dune Analytics、TronExplorer」_January 2025

2. Research on Illicit Use of Stablecoins

2.5 Step Three of Illicit Use: Cashing Out

Step 3 of illicit use: Cashing out

Cashing out is the act of moving funds to an endpoint such as exchanges usually from clean addresses and converting funds into fiat currency. The techniques used in this step are summarized in the following pages.



	Description
Step1	■ **Activities of accumulation of tokens from crimes such as hackings and scams at specific addresses on the blockchain** • Activities involving **thefts of tokens** using off-chain tools such as websites and social medias, **payments for ransomware or transactions on the dark web**, **tax evasion concealment**, etc. • Activities involving fund transfers from clean addresses to sanctioned addresses.
Step2	■ **Activities aim at disrupting tracking by moving tokens using on-chain laundering techniques** • Activities involving the use of mixing/tumbling services, privacy coins, dapps, DeFi, etc. to launder funds.
Step3	■ Activities of moving funds to an endpoint such as exchanges and cashing out into fiat currency • Activities involving the use of off-ramp services in jurisdictions with lax AML/CFT regulations or knowingly cashing out illicit funds.

Cash-out routes used by illicit actors

For cashing out, there are several methods to off-ramp to fiat, with cryptocurrency exchanges being the most commonly used, but the possibility of using it for payments in the future is also expected to increase.

The final step of money-laundering is to cash out into fiat currency (off-ramp) through seemingly legitimate routes and escape.

Cryptocurrency exchanges

- Cryptocurrency exchanges function as crucial gateways between fiat currency and cryptocurrency. Illicit actors often use exchanges as a laundering endpoint just before withdrawing to fiat currency, taking advantage of its link with traditional financial institutions such as banks.
- By bypassing the KYC/CDD processes of regulated exchanges or using unregulated exchanges or those in countries/regions with lax regulations, there have been numerous past cases where illicit actors successfully cashed out from exchanges.

Shopping

- Darknet markets are convenient for illicit actors, where they can purchase goods and resell them to generate funds unrelated to the origin.
- Illicit actors target a wide range of items for resale, from easily sellable items such as luxury goods, gift cards, and electronics to high-value items such as real estates, vehicles, arts, watches, and jewelries.
- With the potential widespread adoption of stablecoins as a payment method, the possibility of illicit actors purchasing goods from legitimate merchants and reselling them to cash out may increase.

DeFi

- Due to the lack of regulation related to DeFi, many DeFi platforms do not have KYC process. Illicit actors can use these platforms to leverage funds as collateral and convert them into legitimate funds.

Cryptocurrency ATMs

- Cryptocurrency ATMs provide bi-directional exchange services between fiat currency and cryptocurrencies, thus offer the convenience of directly withdrawing fiat currency.

Wallets without KYC

- Non-custodial wallet services often do not require KYC, making them susceptible to being exploited as channels for transfers and payments during the final cash-out stage by illicit actors.

Other platforms

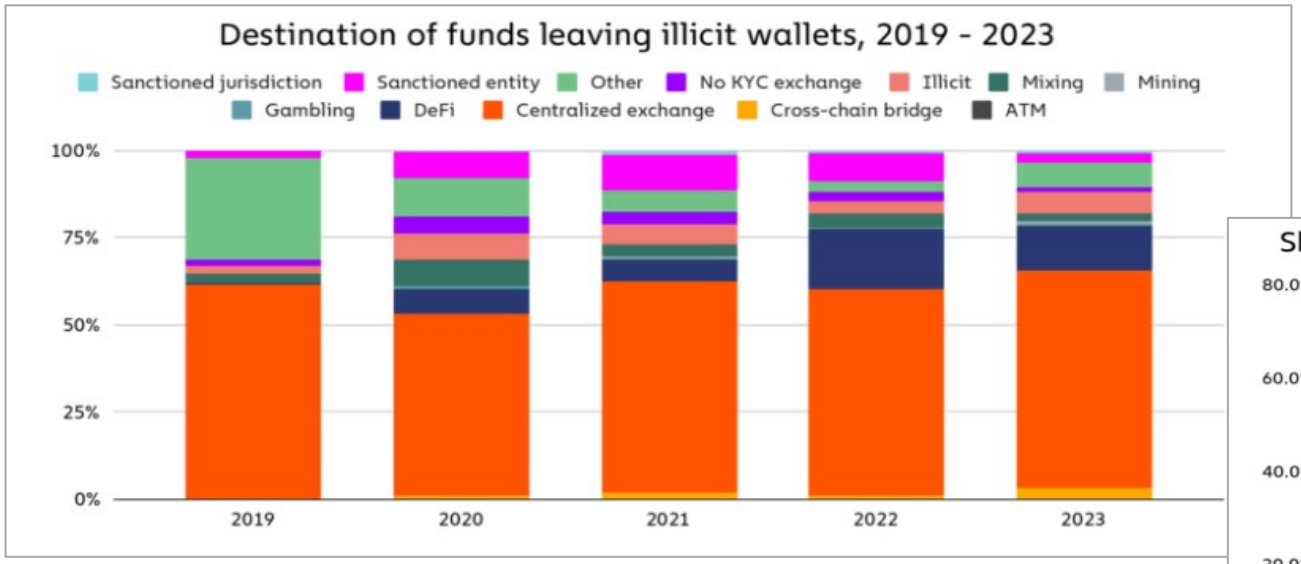
- Illicit actors may also use P2P platforms, gambling services, etc. to convert illicit funds into legitimate ones and cash out.

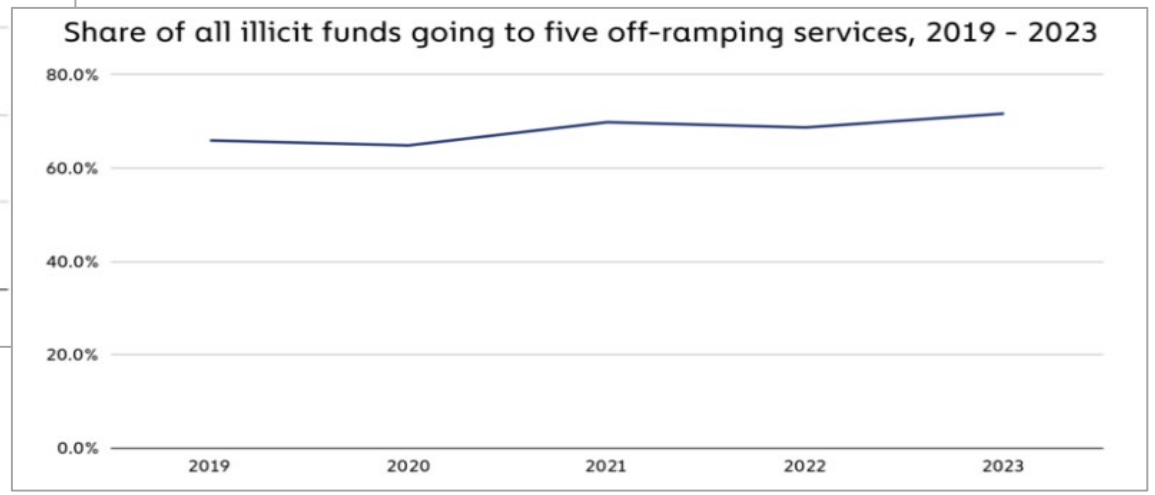
...

High concentration in use of off-ramp services

Centralized exchanges are noted to be the primary receivers of illicit funds, with criminals tending to prefer major platforms when choosing off-ramp services.

Overall, centralized exchanges remain the primary destination for funds sent from illicit addresses, at a rate that has remained relatively stable over the last five years. **Of all illicit funds sent to off-ramping services in 2023, 71.7% went to just five services.**





【Source】：「Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group」（Chainalysis）_March 2025

Money-laundering through exchanges

Crypto exchanges are being abused in a variety of ways by illicit actors.

Not fully regulated

Unlicensed Exchanges

- Considering that unlicensed and non-compliant exchanges often do not require any KYC or customer due diligence (CDD) information from users, criminals can operate under a veil of additional anonymity.
- In addition, some non-compliant and unlicensed exchanges have **themselves been criminal enterprises** and deliberately facilitated illicit activity.

Exchanges in high-risk jurisdictions

- **Criminals will often look to exchanges that are in high-risk jurisdictions** during the money laundering process. This can include:
  - countries and regions that are generally high risk for money laundering and terrorist financing purposes.
  - countries subject to international financial sanctions, embargoes and other restrictions;
  - countries on the FATF's list of High Risk and Non-Cooperative Jurisdictions; and
  - countries with no AML/CTF regulation around cryptoassets, or with ineffective regulatory frameworks.

【OTC Traders Operating on Exchanges】

- Over-the-Counter (OTC) brokers facilitate large trades between liquidity providers, often at lower prices than those available on exchanges. Their large trades offer a convenient cover for the introduction of illicit funds.
- By **maintaining nested accounts at larger exchange businesses**, illicit OTC brokers can conceal themselves in the larger cryptoasset ecosystem with a veneer of legitimacy. These OTC services may also offer crypto-to-cash swaps for users without seeking KYC information.

Regulated

Legitimate Exchanges

- Legitimate exchanges can have a "mixing" effect for criminals. **They can obtain new, untainted coins or cash out with fiat so that their otherwise tainted trail of activity appears clean**.

【Bypass AML controls using KYC kits】

- Sold on the dark web, KYC kits provide criminals with stolen identity details of victims that can be used to open accounts and bypass AML controls. KYC kits can include a significant amount of information about the victim, such as full name, date of birth, residential address, images of ID documents with photo.

【Money Mules】

- In this scheme, victims (the Money Mules) such as university students respond to job advertisements on social media, then get instructed by the criminal organization to open accounts at exchanges using their identity details and documents. The criminal organization would then instruct them to transfer the funds.

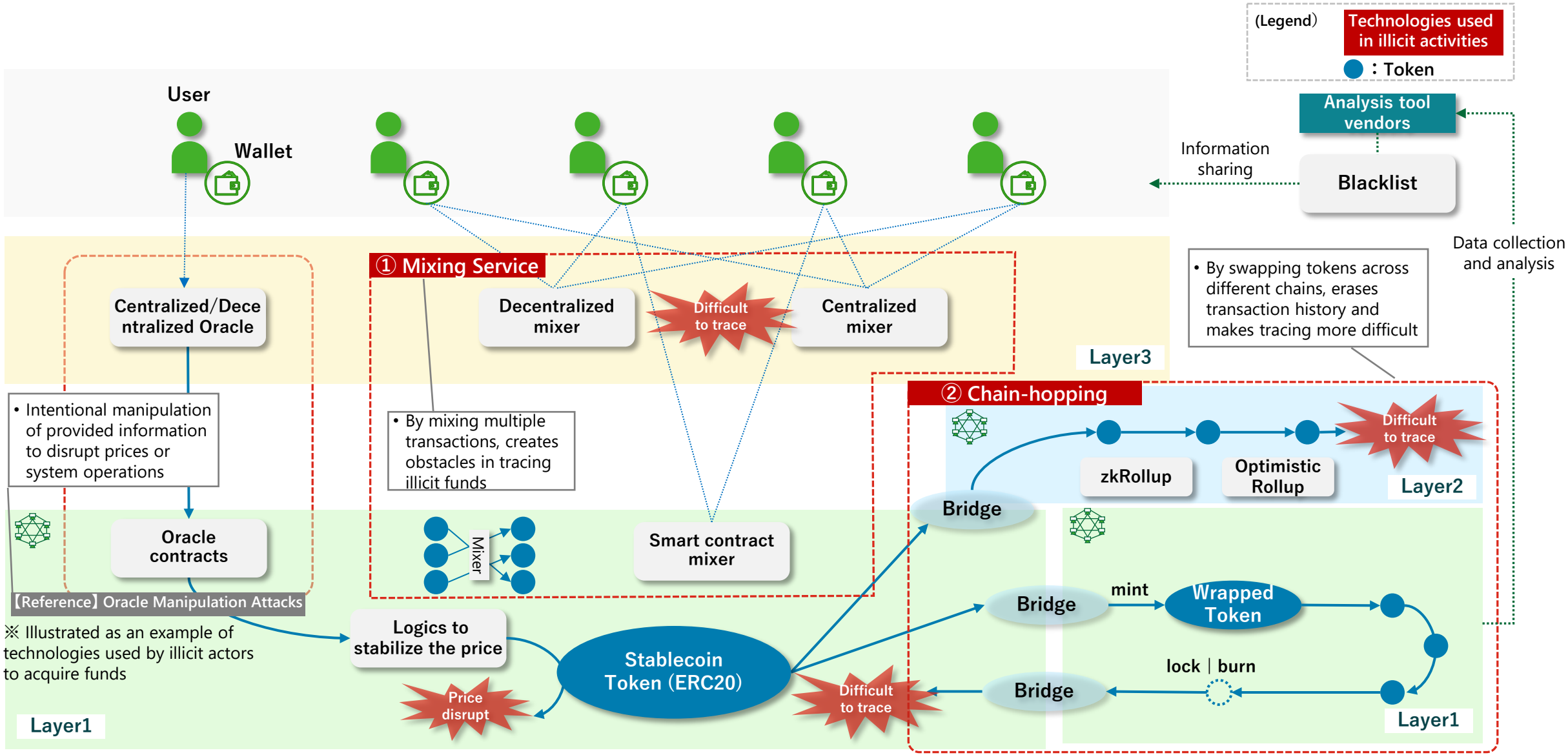
【Source】:「Elliptic Typologies Report 2024 - Preventing Financial Crime in Cryptoassets : Identifying Evolving Criminal Behavior」（Elliptic） _March 2025

2. Research on Illicit Use of Stablecoins

2.6 Technological Trends and Countermeasures

Technologies used for laundering illicit stablecoins

Technologies used for laundering include mixing, which conceals theft routes, and chain-hopping across multiple chains.



Technologies used in laundering crypto-assets and approaches to address them

Addressing technologies such as mixing, which conceals theft routes, and chain-hopping across multiple chains, further cooperation between issuers and analysis companies is necessary for crime tracking and prevention.

#	Technologies used illicitly	Approaches to address the problem	Challenges	Related protocols
①	■ **Mixing, which conceals the route of fund transfers** ➢ Conceal route of fund transfers by mixing transactions of multiple users, withdrawing to different addresses, and moving to different accounts or chains	■ **Sanction the addresses and smart contracts of mixing service providers and check the sanction list at the time of transaction** 【Countermeasures by actor】 • Issuers: Implement monitoring, tracking, and censorship functions, Restrict the use of mixing services • Service providers/Users: Check suspicious counterparties and sanction lists provided by analysis tool vendors, send alerts to users in wallets	■ How to ensure implementation of screening suspicious counterparties and sanction lists ■ How to analyze and distinguish illicit transactions from regular transactions with advanced techniques (e.g., Coinjoin)	• Centralized mixers (e.g., Blender.io) • Decentralized mixers (e.g., Coinjoin) • Smart contract-based mixers (e.g., Tornado Cash)
②	■ **Chain-hopping, which launder stablecoins through different chains, such as Layer2** ➢ Make tracking difficult by bridging illicit funds across multiple chains in a short time, using different wallets for each chain, and eventually cashing out to fiat currency through cryptocurrency exchanges or OTC/P2P transactions ➢ Make tracking difficult by bridging illicit funds to Layer2 (L2) which is designed for scalability and fee reduction, and circulating them on L2	■ **Track cross-chain transactions using blockchain analysis tools to graphically analyze information** 【Countermeasures by actor】 • Issuers: Implement monitoring, tracking, and censorship functions with analysis tools • Service providers/Users: Monitor cross-chain transactions with advanced analysis tools and codes such as AI to detect suspicious activities (e.g., Blockaid services)	■ How to collaborate and improve analysis tools, as tracking becomes difficult when involving multiple chains and layers ■ **How to choose from multiple bridging methods, as the optimal implementation of bridge differs for each player**	• Optimistic Rollup • ZK Rollup • Wrapped Tokens • Cosmos/Polkadot • Inter-Blockchain Communication • Cross-Chain Transfer Protocol (CCTP)

Technologies used in laundering crypto-assets and approaches to address them (Reference)

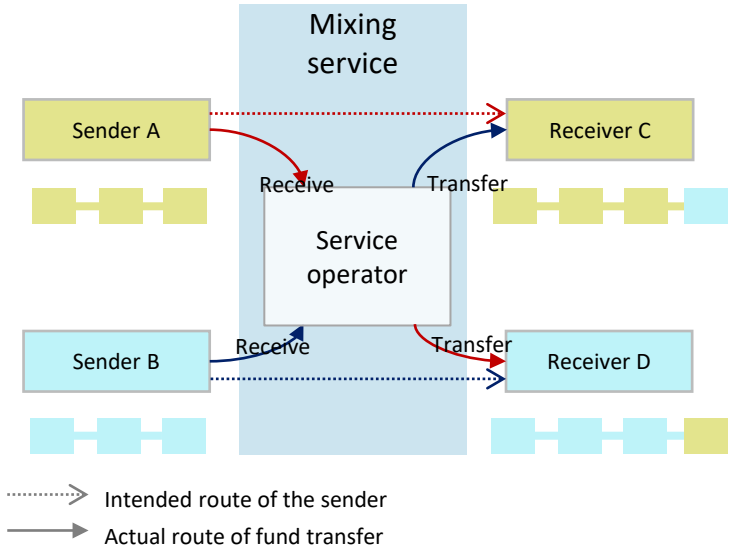
It is possible to enhance censorship and tamper resistance through decentralized oracles by collecting information from multiple data sources.

#	Technologies used illicitly	Approaches to address the problem	Challenges	Related protocols
Ref.	■ **Price manipulation of stablecoins through Oracle Manipulation Attacks on Oracle data** ➢ Disrupt protocol operations to manipulate stablecoin prices by manipulating oracle data with Dapps and sending false information ➢ Primarily used for flash loan attacks, or **price manipulation and arbitrage of algorithmic stablecoins** collateralized by cryptocurrencies	■ **Enhance censorship and tamper resistance through decentralized oracles that collect information from multiple data sources and verify it through consensus.** 【Countermeasures by actor】 • Issuers/Users: — • Service providers: Restrict the use of centralized oracles and introduce decentralized oracles	■ Delays in updates due to consensus formation, difficulty in ensuring consistency of multiple data sources, and system complexity. ■ Lack of regulations or oversights over the community operating the oracle and intermediaries, as it is difficult for issuers/users to detect and act on it.	• Centralized Oracle • Decentralized Oracle

Mixing service

Mixing services are increasingly adopting methods that conceal transactions at the protocol level or combine with other technologies such as Zero-Knowledge Proofs, rather than relying on centralized mixers operating as intermediaries.

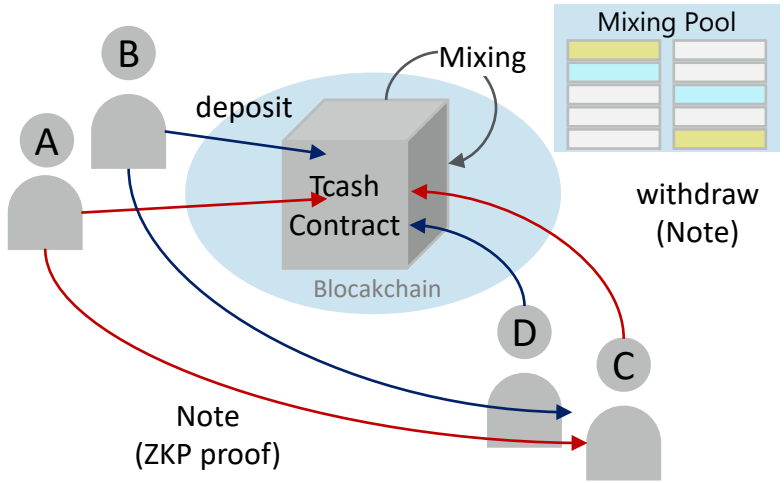
Centralized mixer (Blender.io)



■ **Centralized mixing**

- By mixing funds sent from multiple users in the operator's pool and then transferring these funds to different destination addresses, the relationship between the sender and the receiver is severed, making it difficult to trace.

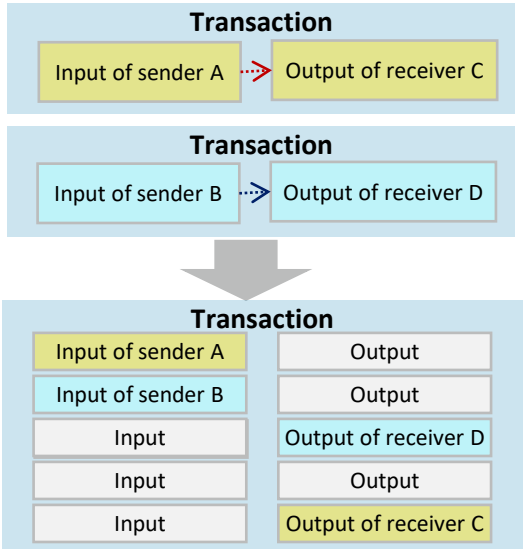
Smart contract mixer (Tornado Cash)



■ **Mixing through smart contract**

- Utilizing Zero-Knowledge Proof (ZKP) to conceal the addresses of the sender and the receiver.
- Users deposit funds into a smart contract, create a secret note containing the ZKP proof, and send it to any address.
- Once deposited, the funds are added to the mixing pool, making it difficult to trace as they are mixed with other transactions.

Decentralized mixer (Coinjoin)



■ **Decentralized mixing**

- Using the UTXO mechanism, this method combines randomly selected transactions (inputs) from other users into a single transaction, making it difficult to identify the real receiver.

■ Centralized mixing and smart contract mixing service providers can be identified by their wallet addresses or smart contract addresses.

■ Although tracking mixed transactions is challenging, transactions or addresses involved in money laundering activities can be identified (by detecting and separating illicit users from legitimate users).

■ **Decentralized mixers, such as Coinjoin, are implemented following basic protocols and are indistinguishable from common transactions.** Consequently, traditional heuristic analysis, which assumes that all public keys used as inputs in the same transaction belong to the same user, cannot be applied.

■ Therefore, more advanced methodologies, such as decomposing transactions into input and output units and using AI to estimate the likelihood of illicit transactions based on each transaction flow, are required.

Chain-Hopping

A money-laundering technique called Chain-Hopping is often used, which enables illicit actors to move illicit funds across multiple blockchain networks.

■ **Chain-Hopping** is one of the most popular money-laundering techniques used by illicit actors in recent years. With new technologies such as cross-chain bridges and wrapped tokens, major blockchains now have interoperability. While this development is convenient for consumers, it has also been a boon for criminals, who can hop from one chain to another to obfuscate their laundering. Investigators now need to track multiple public ledgers, often requiring blockchain analytics tools to graph cross-chain movements. *1

Types of Cross-Chain Bridges *2

■ Lock and mint

- A user locks tokens in a smart contract on the source chain, then wrapped versions of those locked tokens are minted on the destination chain as a form of IOU. In the reverse direction, the wrapped tokens on the destination chain are burned to unlock the original coins on the source chain.

■ Burn and mint

- A user burns tokens on the source chain, then the same native tokens are re-issued (minted) on the destination chain.

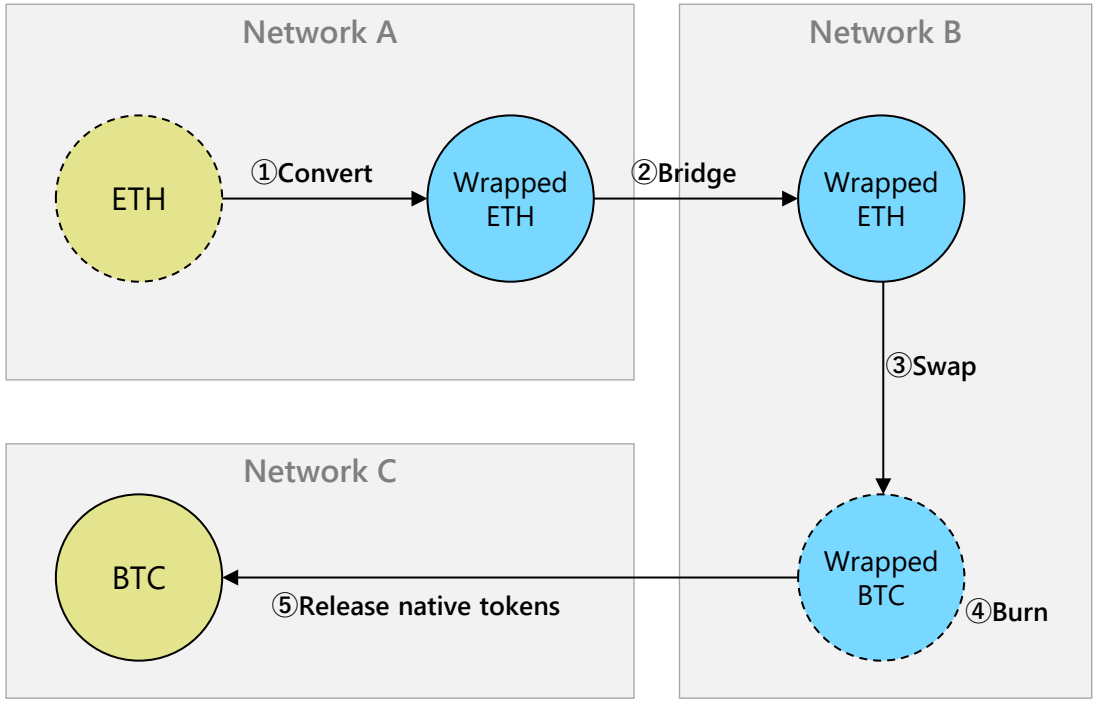
■ Lock and unlock

- A user locks tokens on the source chain, then unlocks the same native tokens from a liquidity pool on the destination chain. These types of cross-chain bridges usually attract liquidity on both sides of the bridge through economic incentives such as revenue sharing.

■ Others

- Programmable token bridges, which involve a combination of token bridging and arbitrary messaging, enable more complex cross-chain functionality. These include swapping, lending, staking, or depositing the tokens in a smart contract on the destination chain in the same transaction that the bridging function is executed.

Chain-hopping example using wrapped tokens *3



【Source】: *1「Money Laundering in Crypto: How Criminals Hide Their Tracks」(MERKLE SCIENCE) _March 2025
*2「What Is A Cross Chain Bridge?」(Chainlink) _ March 2025
*3「Chain Hopping in Crypto: How to Track Cross-Blockchain Fund Movement」(Medium) _ March 2025

[Reference] Emerging technologies in AML/CFT

For stablecoin or other cryptocurrency transactions, new protocols that balance privacy protection with AML/CFT requirements are emerging.

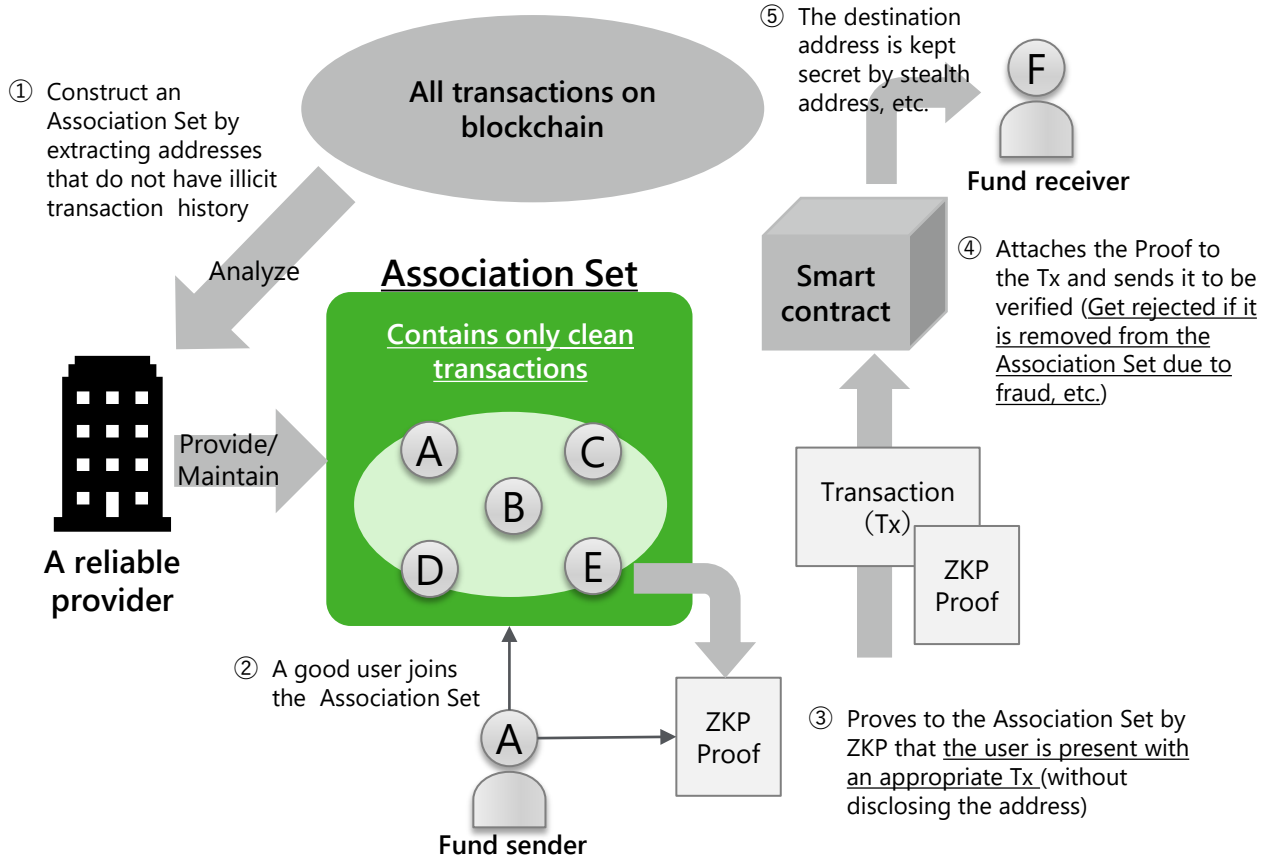
- Technologies to detect and exclude illicit users from good ones in stablecoin or other cryptocurrency transactions, are emerging.
- Traditionally, the focus has been particularly on privacy protection, mainly concealing user's transaction history and balance from third parties. However, technologies that balance privacy protection with monitoring and excluding illicit activities/users from the community and aim to build a more secure and reliable economy, are being considered.
- There is a growing anticipation for practically implementing those technologies, while certain challenges remain, such as the line between legal and illegal activities, the definition of 'reliable providers', and the way of verification which is mostly based on past performance.

#	Technology	Overview	Use case for stablecoins	Challenges
①	**Privacy Pools**	■ **A smart contract-based privacy-enhancing protocol using Zero-Knowledge Proof to separate good users from illicit users** • It suggests that AML/CFT countermeasures can be implemented in mixing services such as Tornado Cash.	➢ Can be used in fund transfer scenario to prove that the sender and receiver are not acting maliciously and are clean. ➢ Users can **prove their compliance without disclosing their entire transaction history**.	• Users may disclose other users' transaction information in order to prove himself legitimate, thereby violating the privacy of others • Malicious providers may build the Association Set to obtain user information (The definition of 'reliable provider') • Determining the logics for extracting clean addresses • Reaching consensus with FATF and regulatory authorities
②	**Accountable Wallet**	■ **A mechanism to prove non-involvement in illicit activities while protecting wallet owners' privacy** • It uses zero Knowledge Proofs to verify the legitimacy of transactions and cross-checks with sanction lists, along with monitoring and reporting of illicit addresses through decentralized oracles.	➢ Can be used to **assess legitimacy of the wallet's ownership, past transactions and the origin of cryptocurrencies.** ➢ Users can check the reliability of their transaction counterparties and prevent getting involved in illicit activities.	• Minimizing the cost of verifying the legitimacy of the transaction counterparty • Determining logics for the credit scoring (by advanced blockchain analysis and manual collection of transaction details, etc.) • Definition of 'reliable provider' and the standards for issuing credentials

[Reference] Privacy Pools

Privacy Pools is a fund transfer protocol in which users can prove their compliance by separating themselves from illicit addresses and illicit funds.

- Mixing service such as Tornado Cash can hide the true routes of fund transfers, making it very difficult to clearly distinguish good transactions from bad transactions by "undesirable individuals or groups“ that intend for money laundering.
- **Privacy Pools is a mechanism to protect user privacy while proving that the user was not involved in illicit funds in past transactions.**



Comparison with Tornado Cash

Items	Privacy Pools	Tornado Cash
Purpose	• Privacy + Compliance	• Complete privacy
How anonymization works	• Using an Association Set, allow only clean transactions	• Mix transactions for all users
Zero Knowledge Proof (ZKP)	• Used for proving a clean transaction history	• Used for hiding the relationship between sender and receiver
Elimination of illicit transactions	• Possible (by maintaining the Association Set)	• Impossible (for anyone can use the service)
Compliance	• Easy to comply with regulations (by cooperating with exchanges, authorities)	• No compliance (and is sanctioned by OFAC)

Challenges in practicing Privacy Pools

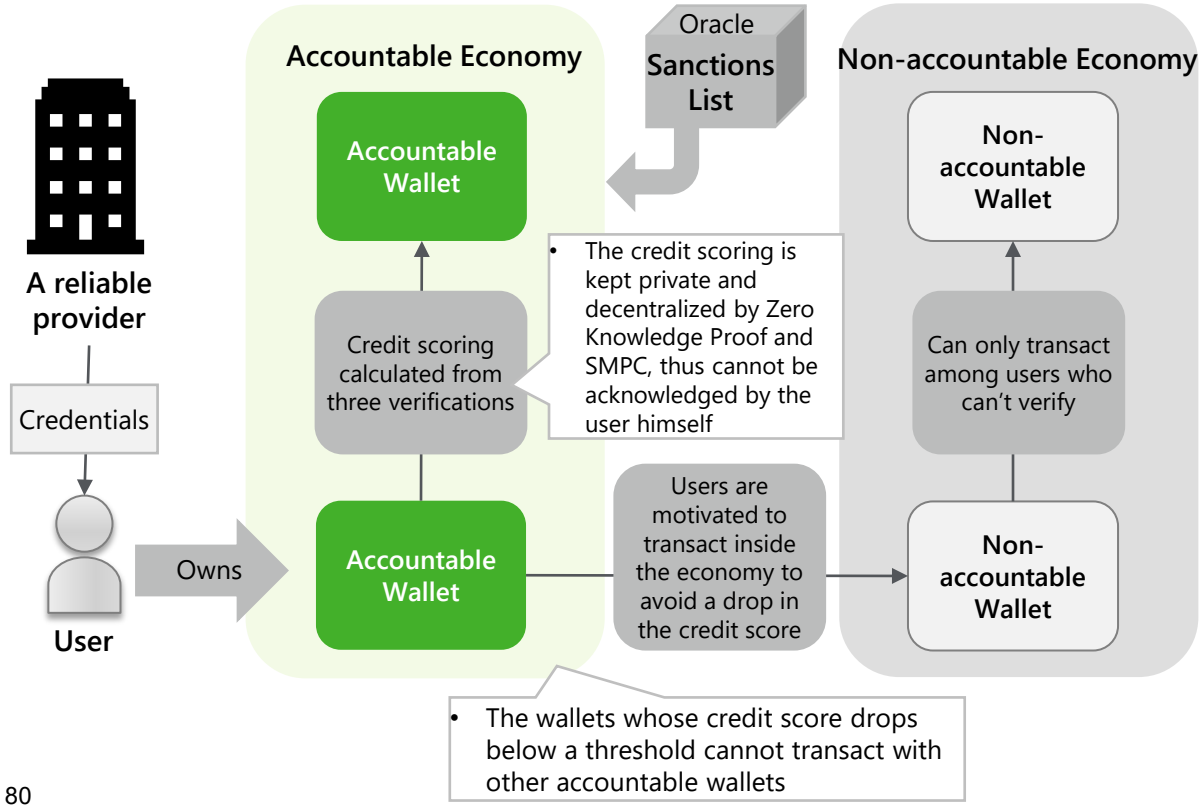
- Users may disclose other users' transaction information in order to prove himself legitimate, thereby violating the privacy of others
- Malicious providers may build the Association Set to obtain user information (The definition of 'reliable provider')
- The logics for extracting clean addresses need to be determined

[Reference] Accountable Wallet

Accountable Wallet is a mechanism aiming to determine and build an Accountable Economy based on the credit score calculated from several aspects.

- Accountable Wallet defines clear criteria for evaluating the legitimacy of transactions and **provides a comprehensive approach to ensure the safety, transparency, and compliance of transactions** in decentralized finance (DeFi).
- Specifically, by credit scoring based on three verifications on the wallet's ownership, past transactions and the origin of cryptocurrencies, it aims to **determine and build an Accountable Economy based on the credit score**.

Accountable Framework



Three verifications of Accountable Wallet

- **Legitimacy of ownership**
  - Proof that the wallet owner is not part of any anti-social forces or subject to sanctions. This includes credentials digitally signed and issued by a reliable provider, based on the wallet owner's personal information
- **Legitimacy of past transactions**
  - Proof that the wallet has not been involved in illicit activities in the past. This includes non-membership proof verifying that the wallet is not listed on sanction lists or cryptocurrency watchlists.
- **Legitimacy of the origin of cryptocurrencies**
  - Proof that the wallet has not received cryptocurrencies obtained illicitly in the past. This includes chain certificates showing that the sources of received cryptocurrencies are legitimate, and these certificates are generated based on past transaction history.

Challenges in practicing Accountable Wallet

- Minimizing the cost of verifying the legitimacy of the transaction counterparty
- Determining logics for the credit scoring (by advanced blockchain analysis and manual collection of transaction details, etc.)
- Definition of 'reliable provider' and the standards for issuing credentials

3. Research on Major Stablecoin Issuers

3.1 Overview (USDT/USDC)

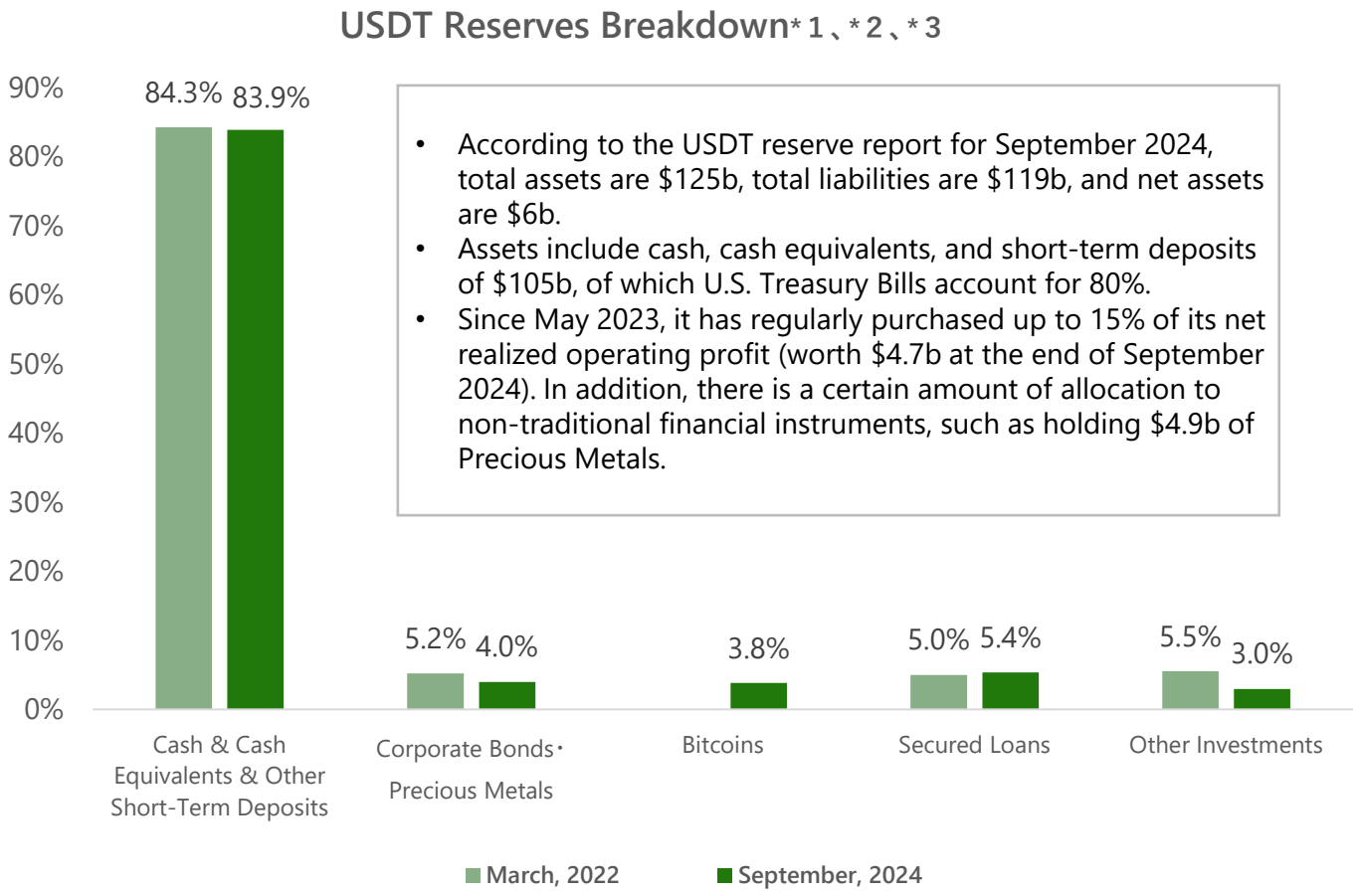
Overview and key updates of USDT

Tether's market capitalization has grown significantly since 2022, however, there are some issues that need to be addressed, such as the delisting of USDT by CEX in Europe due to the impact of MiCA regulations.

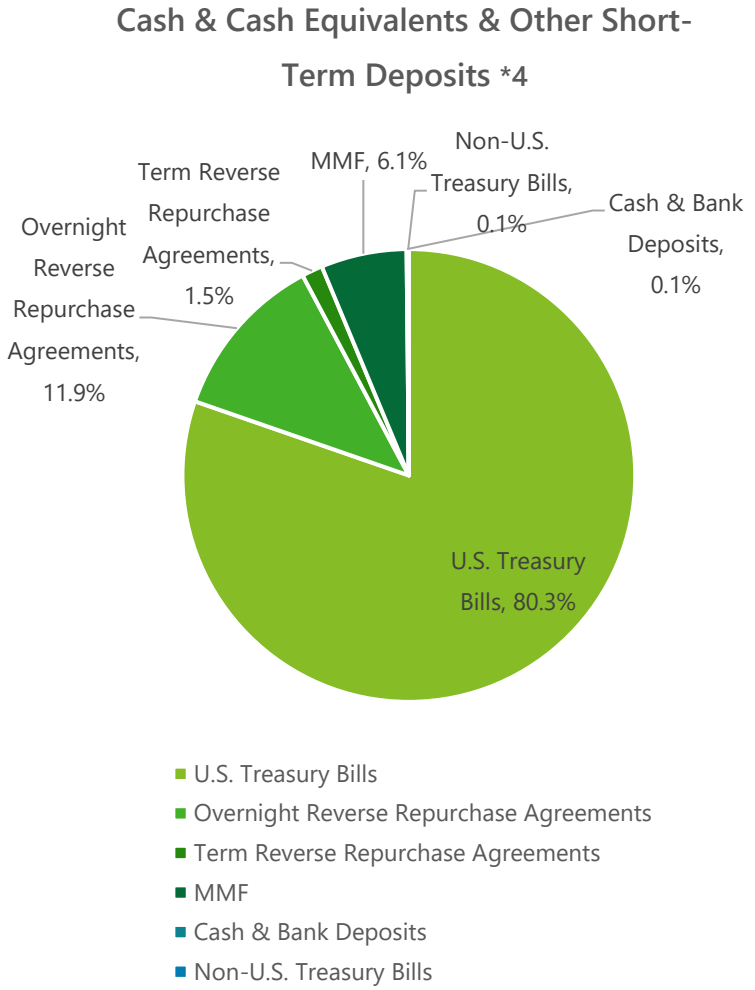
#	Item	Summary of the 2022 Report *1	Key Updates *2
(1)	Business model	■ USDT is a crypto asset pegged to fiat currency and issued by Tether Operations Limited or its affiliates (Hereinafter collectively referred to as "Tether"). Initially launched on the Bitcoin blockchain, it now functions as a second layer product on the blockchain of Ethereum, EOS, TRON, and Argorand, the hash algorithms of which are used.	■ Market cap more than doubled from $65 in July 2022 to $140 in December 2024 ■ Support 15 blockchains as of the end of 2024, increased from 12 in July 2022 ✓ Newly launched on: NEAR Network (in September 2022), Polygon (in May 2023), Aptos (in August 2024) ✓ Will discontinue support for: Kusama, Bitcoin Cash SLP, Omni Layer, EOS, Algorand (in September 2025)
(2)	Business objectives and targeted customers	■ According to Whitepaper, Tether has the following advantages: A) Business objectives • Can operate in anonymous and decentralized P2P networks • Can easily integrate with other operators, crypto exchanges and wallets B) Targeted customers • Both individual and business users can use Tether services	■ Tether's efforts to comply with the requirements of regulators ✓ In 2023, Tether actively cooperated with the Department of Justice, the US Secret Service and the Federal Bureau of Investigation (FBI), which led to the blocking of USDT worth a total of $435 million. Tether also announced the launch of a new policy to freeze wallets belonging to individuals sanctioned by the Office of Foreign Assets Control (OFAC). *3 ■ Announced in November 2024 that Tether would invest in StablR and discontinue support for EUR₮, considering the evolving regulatory frameworks surrounding stablecoins in the European market ✓ StablR offers two coins: EURR and USDR, both issued on Ethereum and Solana. In July 2024, StablR secured an Electronic Money Institution (EMI) license authorized by the Malta Financial Services Authority, for its MiCAR-compliant stablecoins. ■ Due to the impact of MiCA, delisting of USDT in European market has led to market cap falls ✓ Several EU-based crypto exchanges and Coincase delisted Tether's USDT to comply with MiCA regulations, resulting in market cap falls. (January 2025)
(3)	Procedures and conditions for issuance and redemption	■ Fees ✓ Deposit fee: 0.1%, minimum amount: $100,000 ✓ Withdrawal fee: $1,000 or 0.1% of redemption, minimum amount: $100,000. Tether deposits and withdrawals are free of charge. ■ Redemption disclaimer ✓ Tether reserves the right to delay the redemption or withdrawal of Tether Tokens if such delay is necessitated by the illiquidity or unavailability or loss of any Reserves.	■ November 2024, Tether announced the launch of Hadron, a platform for issuing and managing the full life cycle of digital tokenized assets ✓ Designed to simplify the tokenization of everything from stocks to bonds, stablecoins, loyalty points, and more ✓ Seamless user experience for token issuance and redemption ✓ Provide comprehensive set of tools for compliance, Know-Your-Customer (KYC), Anti-Money-Laundering (AML), etc.

Overview and key updates of USDT - Reserves

Most of Tether's reserves are low-risk assets, but they have a policy of holding a certain degree of risk assets.



- According to the USDT reserve report for September 2024, total assets are $125b, total liabilities are $119b, and net assets are $6b.
- Assets include cash, cash equivalents, and short-term deposits of $105b, of which U.S. Treasury Bills account for 80%.
- Since May 2023, it has regularly purchased up to 15% of its net realized operating profit (worth $4.7b at the end of September 2024). In addition, there is a certain amount of allocation to non-traditional financial instruments, such as holding $4.9b of Precious Metals.



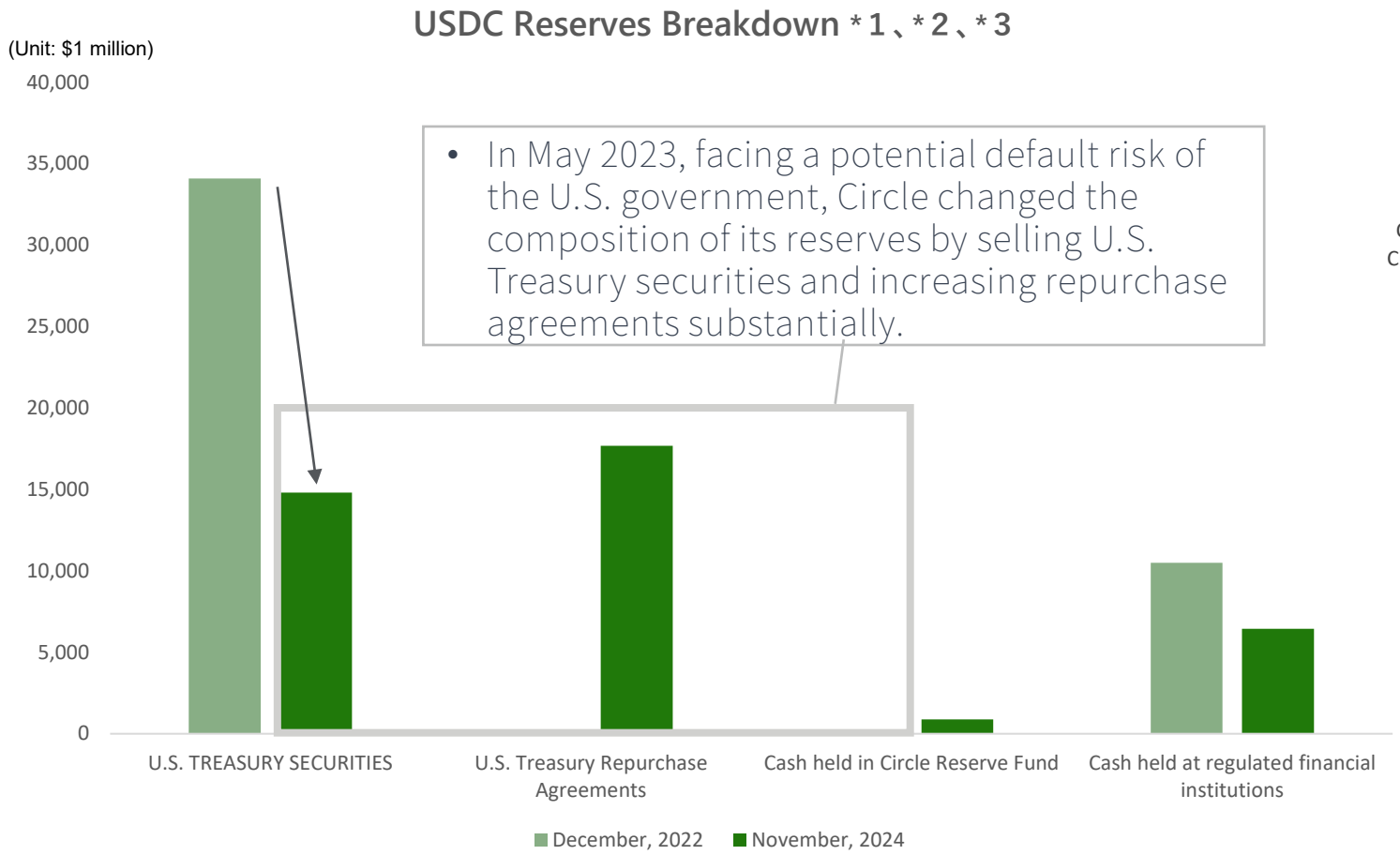
Overview and key updates of USDC

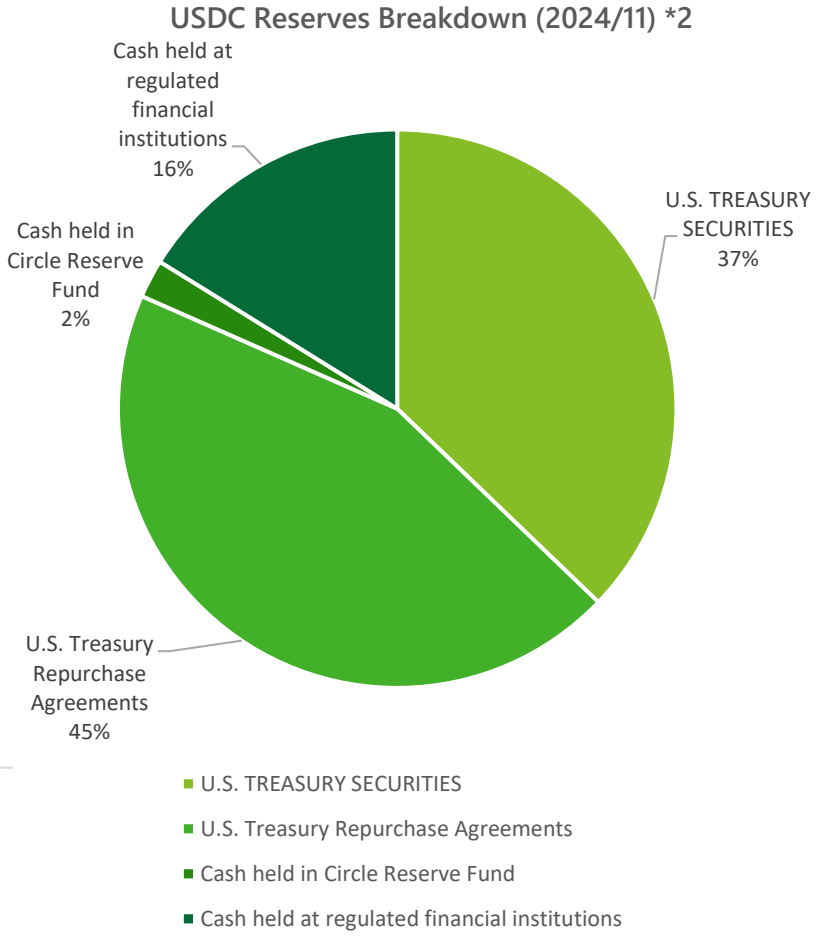
Since 2022, Circle has been expanding its business schemes and customer targets by adding blockchains and complying with MiCA regulations.

#	Item	Summary of the 2022 Report *1	Key Updates *2
(1)	Business model	■ USDC is a crypto asset issued according to standards designed by the Centre Consortium, which was established jointly by Coinbase and Circle. It is a scheme assuming that multiple issuers can exist. Each USDC is backed by reserves and is redeemable at $1.	■ Governance of USDC shifted from Centre to Circle ✓ Announced in August 2023, Circle shut down the separate governance body Centre, the jointly managed operator of USDC with Coinbase, and Circle take full control over USDC issuance and governance. ■ Support 16 blockchains as of the end of 2024, increased from 8 in September 2022 ✓ Newly launched on: Arbitrum One, NEAR, Optimism, Polkadot (in 2022); Cosmos, Bas, Polygon (in 2023); Celo, Zksync, Sui (in 2024) ✓ Discontinued support for: Tron (in February 2024), Flow (in August 2024)
(2)	Business objectives and targeted customers	■ By completing KYC process, business users can purchase USDC through their Circle account ■ To create a Circle account, the business user need to enter the company's name and its representative's information. Individual users can only buy USDC at crypto exchanges.	■ In July 2024, Circle launched USDC and EURC issuance in Europe and became the first global stablecoin issuer to comply with MiCA ✓ Circle attained an Electronic Money Institution (EMI) license from the Autorité de Contrôle Prudentiel et de Résolution (ACPR), the French banking regulatory authority, in compliance with MiCA. ■ Circle's continue efforts to acquire licenses globally ✓ In June 2023, Circle obtained Major Payment Institution (MPI) license in Singapore
(3)	Procedures and conditions for issuance and redemption	■ There is no issuance fee free (subject to US dollar wire transfer), nor redemption fee. ■ However, users may be charged by the receiving bank. According to the USDC Terms, redemption is conditional on (i) your possession of a corresponding amount of USDC associated with a registered Circle Mint account, (ii) no violation of these Terms or your Circle Mint account User Agreement, and (iii) no action, pending or otherwise, by a regulator, law enforcement or a court of competent jurisdiction that would restrict redemption	■ From February 2024, Circle provides Standard and Basic options for USDC's redemption ✓ Standard redemption: free for redeeming up to $15 million a day, amounts above $15 million will incur a 0.1% fee. ✓ Basic redemption: fee-free regardless of transaction volume, however, processing can take up to two business days. ■ In October 2024, Circle revised Standard redemption fees and charge for redemptions greater than $2 million a day ✓ Standard redemption: free for first $2M net /day; a fee of .03% will be charged for redemptions greater than $2M, .06% for redemptions greater than $5M, and .1% for redemptions greater than $15M. ✓ Basic redemption: no change.

Overview and key updates of USDC - Reserves

Circle announced that since May 2023, they have increased the proportion of repo transactions as a countermeasure against the potential default of the U.S. government.





Stablecoin Stability Assessment by S&P Global Rating

S&P noted that while USDT's price has remained relatively stable, its disclosure has limited transparency, and that USDC benefits from a clear and transparent approach for the management of its underlying assets.

Item	USDT	USDC
Summary	• Issued in 2014, USDT is the longest-standing stablecoin with the largest volume in circulation. It is issued by Tether International Ltd. and Tether Ltd., which are incorporated in the British Virgin Islands (BVI) and Hong Kong, respectively. Both are wholly owned by British Virgin Islands-registered Tether Holdings Ltd. • Its price has remained relatively stable in recent years, however, asset assessment of 4 (constrained) reflects a lack of information disclosure. Other weaknesses have been observed, including limited transparency on reserve management and risk appetite, lack of a regulatory framework, no asset segregation to protect against the issuer's insolvency.	• USDC is a fully fiat-collateralized stablecoin first issued in September 2018 by Circle. USDC benefits from full backing by low-risk assets, primarily short-dated securities and deposits with banks. • Circle is registered with the Financial Crimes Enforcement Network (FinCEN), a department of the U.S. Treasury, showing some state oversight.
Asset assessment *	**4 | Constrained** • A large share of USDT's reserves comprise highly liquid and secure assets such as short-term U.S. Treasury bills and similar cash equivalents. • Its reserve report does not disclose any information about the creditworthiness of the entities that act as custodians, counterparties, or bank account providers of the assets in the reserve. Money market funds make up 5% of the underlying assets, but there is no publicly available information on those funds.	1 | **Very strong** • USDC benefits from full backing by low-risk assets, primarily short-dated securities and deposits with banks. • Its reserves consist primarily of treasury debt and U.S. treasury repurchase agreements held at the CRF, which is an SEC-registered fund and managed by BlackRock.
Stablecoin stability assessment *	**4 | Constrained** • The stablecoin stability assessment of 4 (constrained) relates to the abovementioned disclosure with limited transparency, in particular. • There is also significant exposure to higher-risk assets, such as precious metals, secured loans and Bitcoin. The stablecoin stability assessment could worsen if there is a shift to higher-risk assets. • Although USDT is registered with the Financial Crimes Enforcement Network (FinCEN), Tether International Ltd. and Tether Ltd., the issuer entities of USDT, are not subject to regulation or supervision by an authoritative body.	**2 | Strong** • USDC benefits from a clear and transparent approach for the management of its underlying assets. Circle publishes information about the composition of assets on its website with a high update frequency. The assets are also subject to monthly attestation and monthly review by an independent auditor. • Its reserves consist primarily of low-risk assets, and the secondary market liquidity for USDC is strong. • Circle, the issuer entity of USDC, is regulated by FinCEN in U.S., and by the U.K. Financial Conduct Authority (FCA) as an Electronic Money Institution.
Adjustment *	**0 | Neutral** • No adjustment was made to the asset assessment despite certain weaknesses such as limited transparency on reserve management, which commensurate with a stablecoin stability assessment of 4 (constrained).	**-1 | Negative** • This adjustment of -1 (negative) incorporates the view of a lack of certainty regarding the bankruptcy remoteness of the collateral assets from Circle more broadly. • Circle notes that USDC reserves are segregated and shielded from Circle creditors in the event of a Circle bankruptcy. However, at this time there is insufficient precedent or certainty that these reserves would be considered separate from the rest of Circle's business and operations.

【Source】：「USDT Stablecoin Stability Assessment」（S&P Global Ratings）_Dec. 2024,「USDC Stablecoin Stability Assessment」（S&P Global Ratings,）_Dec. 2023

*Asset assessment and Stablecoin stability assessment are assessed on a scale of 1-5, where 1 is very strong and 5 is weak. Stablecoin stability assessment is based on the Asset assessment result and adjusted by an indicator of -1(Negative) / 0 (Neutral) / 1 (Positive).

3. Research on Major Stablecoin Issuers

3.2 Promotion Activities of Stablecoins by Issuers

Promotional Activities (Excerpts from major press releases since April 2022)

USDT primarily targets ancillary services used by individuals in emerging markets, while USDC focuses on core payment services, primarily targeting businesses and financial institutions in developed countries and Asia.

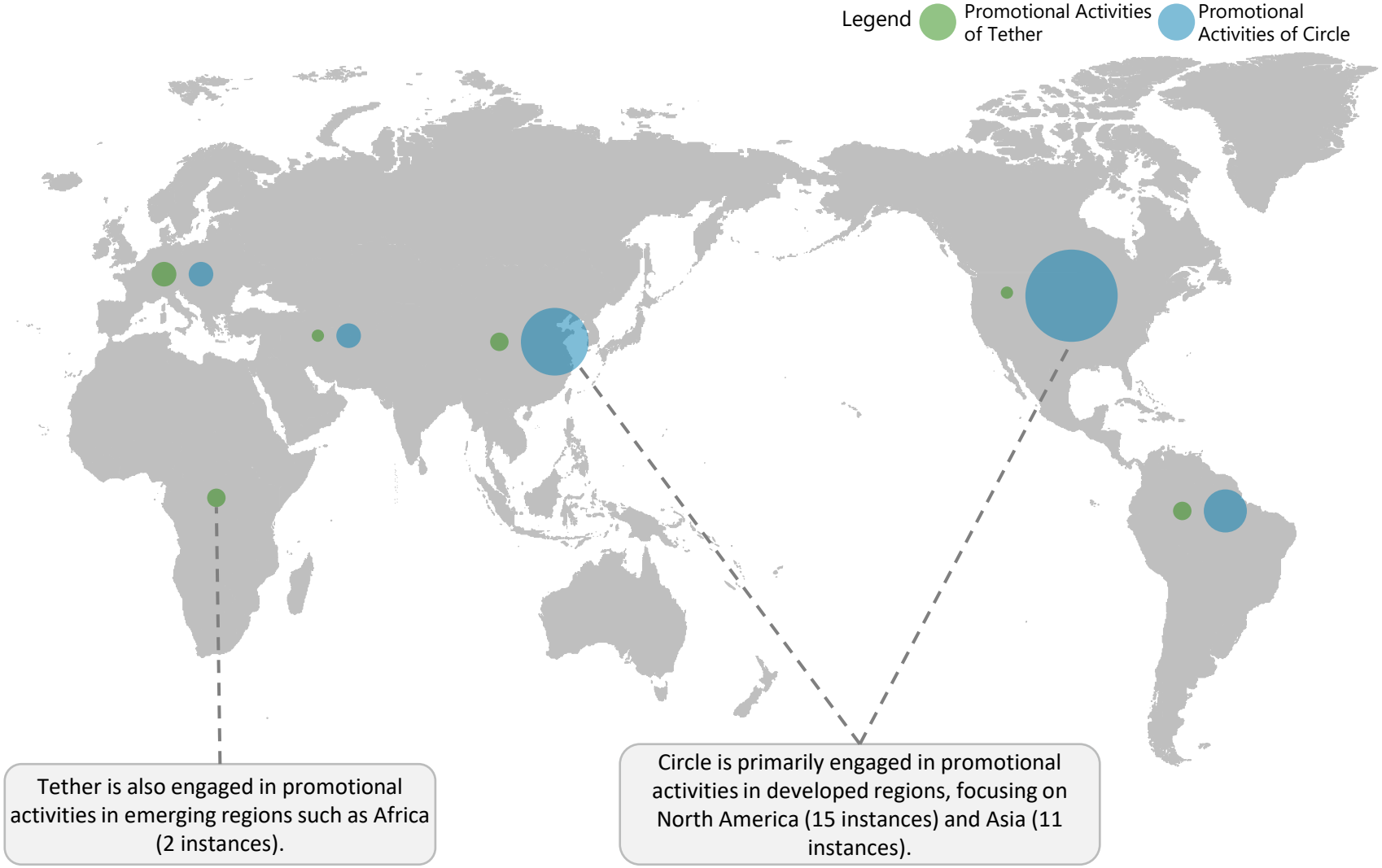
Blue Text: Areas Where Differences Are Observed

項目	USDT	USDC
Overview (Provided Payment Services, Areas, etc.)	■ **The primary focus is on investment and partnerships in payment ancillary services for individuals in emerging markets, with recent activities addressing Europe.** The main regions of operation include North America, Latin America, the Middle East, and Africa.	■ **The primary focus is on investments and partnerships in core payment services for businesses and financial institutions in developed countries and Asia. In 2024, the company will comply with MiCA regulations, with a particular emphasis on early initiatives in Europe.** (Main Regions of Operation) North America, Latin America, the Middle East, Europe, Asia
Investment and Partnership Activities	• February 2025: Announced a strategic partnership with Reelly Tech, a real estate B2B platform in the UAE. • December 2024: Invested approximately $800 million in video-sharing platform Rumble. • December 2024: Invested in MiCA-compliant issuers StabIR and Quantoz Payments to promote operations in Europe. • November 2024: Announced funding for oil trading in the Middle East. • September 2024: Invested $1.5 million in Sorted Wallet, a payment service for individuals in Africa. • August 2024: Invested $3 million in Kem, a payment service app for individuals in the Middle East. • June 2024: Invested $18.75 million in XREX to promote B2B cross-border payments in emerging markets. • December 2023: Invested in the Academy of Digital Industries, an educational platform in Georgia, and CityPay.io, a wallet provider. • June 2023: Partnered with Yellow Card to promote stablecoin education and adoption among young people in Africa. • October 2022: Partnered with SmartPay to provide remittance services for individuals in Brazil.	• February 2025: Announced a partnership agreement with Orico, Aiquitas, and SLASH VISION PTE. LTD. to issue Japan's first BNPL service "Slash Card" backed by USDC. • January 2025: Announced the acquisition of Hashnote and the USYC tokenized money market fund, as well as a strategic partnership with global trading firm DRW. • January 2025: Bison Digital Assets (Bison Bank) partnered with Circle on MiCA-compliant stablecoins. • December 2024: Partnered with Pockyt (USA), a provider of payment systems for merchants, allowing merchants to use stablecoins as an additional option for both deposits and payments. • October 2024: Partnered with BVNK, a provider of payment services for businesses in Europe. • October 2024: Partnered with Thunes, a provider of payment services for businesses in Singapore. • September 2024: Enabled remittances via Brazil's PIX and Mexico's SPEI. • May 2024: Partnered with Brazil's Nubank and BTG Pactual. November 2023: Partnered with SBI Holdings (SBI Shinsei Bank) and Circle. • September 2023: Visa expanded USDC payment capabilities for acquirers. • September 2022: Invested in Elements, a provider of payment systems for merchants. • June 2022: Invested in CYBAVO (Taiwan), which provides highly reliable digital asset management for businesses and financial institutions.
Deployment Chain*1	Ethereum（46.57%）、Tron（41.95%）、BSC（3.77%）、Arbitrum（2.04%）、Avalanche（1.18%）、TON（1.03%）、Solana（0.74%）、Optimism（0.65%）、Polygon（0.54%）、Near（0.38%）、Other（1.15%）	Ethereum（66.55%）、Solana（8.8%）、Base（7.61%）、Hyperliquid（4.59%）、Arbitrum（2.96%）、Polygon（1.74%）、BSC（1.51%）、Avalanche（1.17%）、Noble（1.06%）、Optimism（0.78%）、Other（3.22%）

[Source] Based on "Why use Tether?" (Tether) and "Circle | USDC & Web3 Services for a new financial system" (Circle), as confirmed by our company as of February 2025. *1 Created by our company based on the aggregation of "DefiLlama - DeFi Dashboard" (DeFiLlama) as of January 6, 2025, indicating a total market capitalization of $206 billion, with USDT at $137 billion (67%) and USDC at $45 billion (22%).

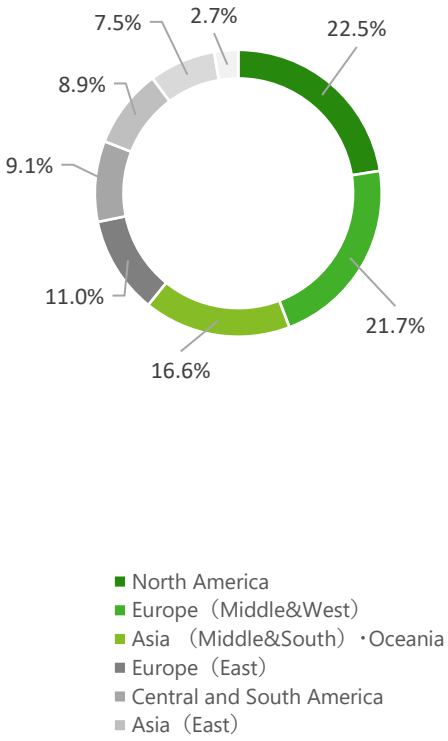
Promotional Activities of Tether and Circle

Tether is engaged in promotional activities in emerging markets, while Circle focuses its promotional activities primarily in developed regions such as North America and Asia.



[Reference] Global Cryptocurrency Trading Share*1

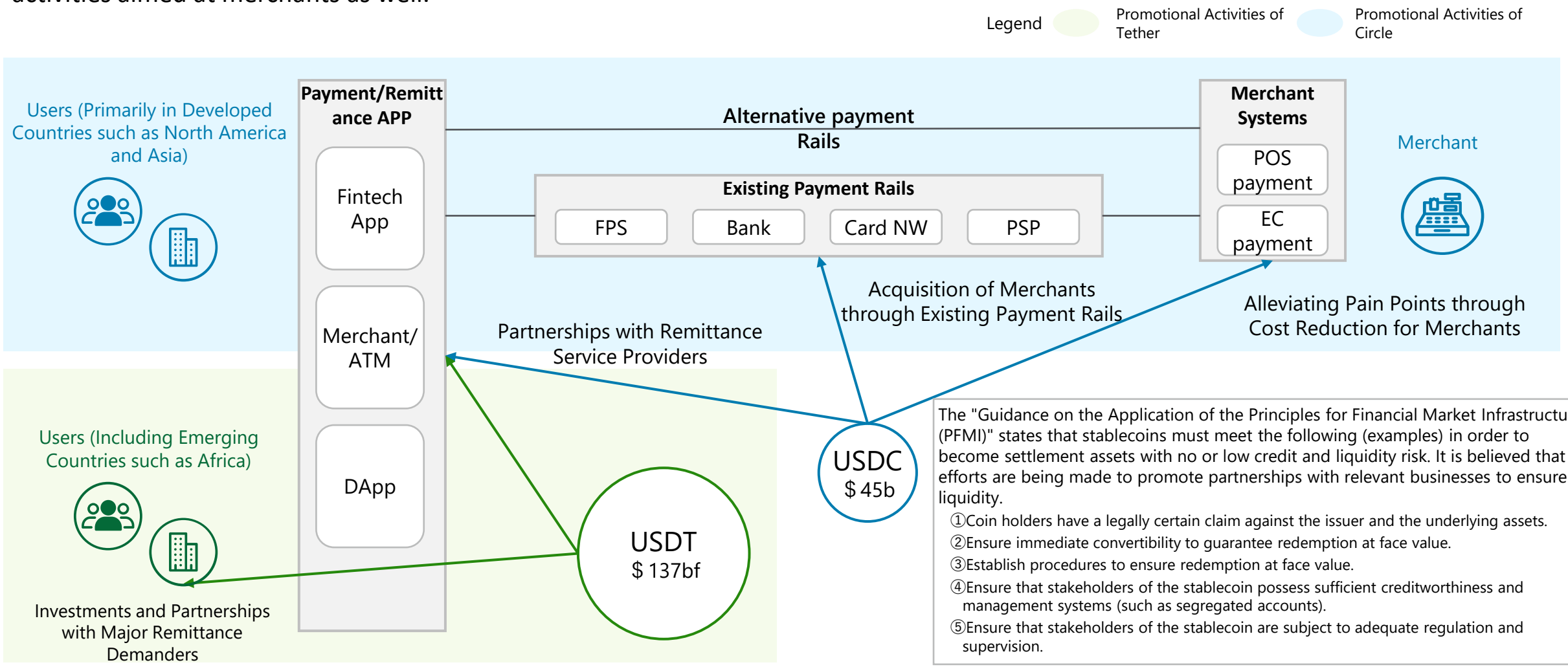
North America, Europe (Central & Western), Asia (Central & Southern), and Oceania together account for approximately 60% of global cryptocurrency trading.



[Reference] Created by our company based on the press releases from "Why use Tether?" (Tether) and "Circle | USDC & Web3 Services for a new financial system" (Circle) during the period from April 1, 2022, to January 21, 2025, as confirmed in February 2025. Also based on the "2024 Geography of Cryptocurrency Report" (Chainalysis) as of February 2025.

Overall Picture of Promotional Activities

Tether is advancing promotional activities directed towards users, while Circle, in addition to user-focused promotional activities, is also engaging in partnerships and investments with existing payment rails and merchant system providers, thereby conducting promotional activities aimed at merchants as well.



The "Guidance on the Application of the Principles for Financial Market Infrastructures (PFMI)" states that stablecoins must meet the following (examples) in order to become settlement assets with no or low credit and liquidity risk. It is believed that efforts are being made to promote partnerships with relevant businesses to ensure liquidity.

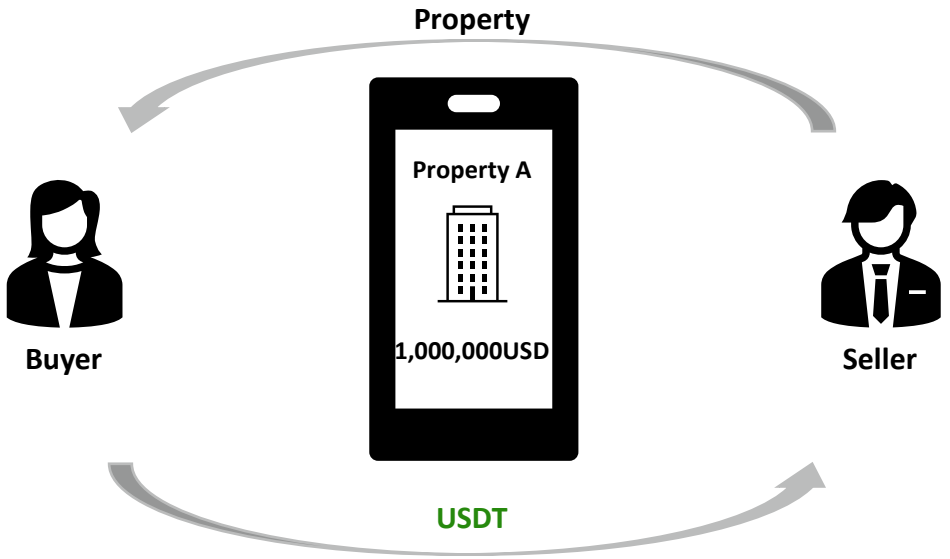
①Coin holders have a legally certain claim against the issuer and the underlying assets.
②Ensure immediate convertibility to guarantee redemption at face value.
③Establish procedures to ensure redemption at face value.
④Ensure that stakeholders of the stablecoin possess sufficient creditworthiness and management systems (such as segregated accounts).
⑤Ensure that stakeholders of the stablecoin are subject to adequate regulation and supervision.

Source: " https://www.boj.or.jp/research/brp/psr/data/psr240910.pdf " (Bank of Japan) Payment and Settlement Systems Report 2024

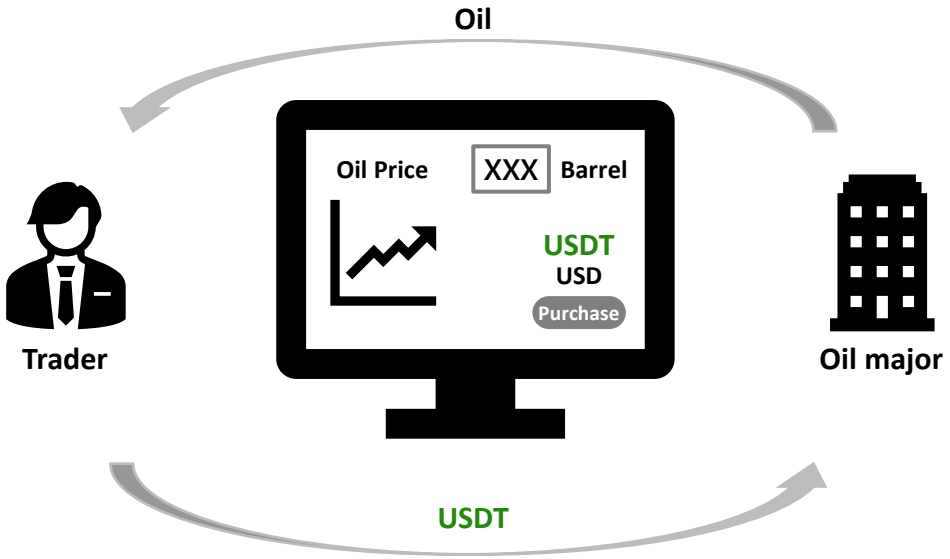
Promotion Activities

In partnerships with large remittance demanders, they have engaged in partnerships and investments for the introduction of USDT settlements in real estate transaction platforms and crude oil transactions.

Promotion Activities for Tether: Partnerships with Major Remittance Demanders

Tether and Reelly Tech Announce Strategic Partnership to Revolutionize Real Estate Transactions in the UAE	
Overview	■ Over 30,000 domestic and international agents on Reelly Tech's platform will leverage the power of USDT to streamline processes and enhance efficiency in one of the jurisdiction's most dynamic markets. ■ The aim is to assist agents in understanding practical applications such as USDT settlements for real estate purchases.
Service Image	

Promotion Activities for Tether: Investment in Major Remittance Service Providers

Announces Funding for Crude Oil Trading in the Middle East	
Overview	■ The investment division announced that it has provided funding for a physical crude oil transaction between a publicly listed major oil company and a top-tier commodity trader. Completed in October 2024, this transaction facilitated the loading and transportation of 670,000 barrels of Middle Eastern crude oil, valued at approximately $45 million. ■ By promoting the use of stablecoin USDT to streamline trade flows, the aim is to bring positive changes to the trade finance industry. ■ The use of USDT in trade finance transactions is being promoted, which will reduce costs and shorten payment times.
Service Image	

Source: Created by our company based on " News - Tether.io" (Tether), confirmed as of February 2025

Promotion Activities

Among existing payment rail companies, Orico has partnered for BNPL using USDC, and merchant system companies have partnered to accept deposits and payments in USDC.

Promotion Activities for Circle: Partnerships with Existing Payment Rails

Agreement Reached for the Issuance of "Slash Card," Japan's First BNPL (Buy Now Pay Later) Service Backed by USDC (USD Coin)

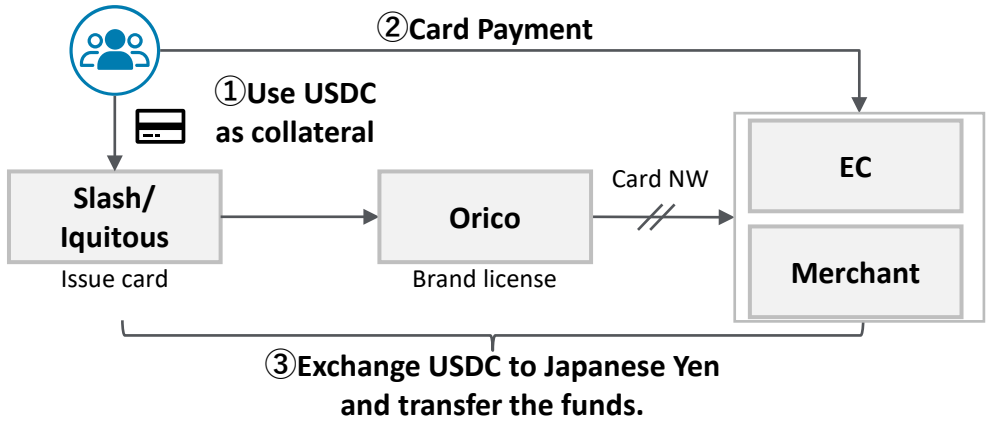
Overview

- By leveraging the stablecoin "USDC" as collateral, we provide a postpaid payment method that combines safety and convenience.
- Users can use their own unhosted wallets to shop at online stores and physical locations, offering a new experience that seamlessly bridges the gap between the world of cryptocurrencies and the real world.

Role of Each

- Orico: Responsible for handling international brand relationships as the BIN sponsor.
- Iquitous: Responsible for customer management and system operations as the card issuer.
- Slash: Responsible for the development, operation, and branding of the "Slash Card" as the program manager and provider of the Slash brand.

Service Image



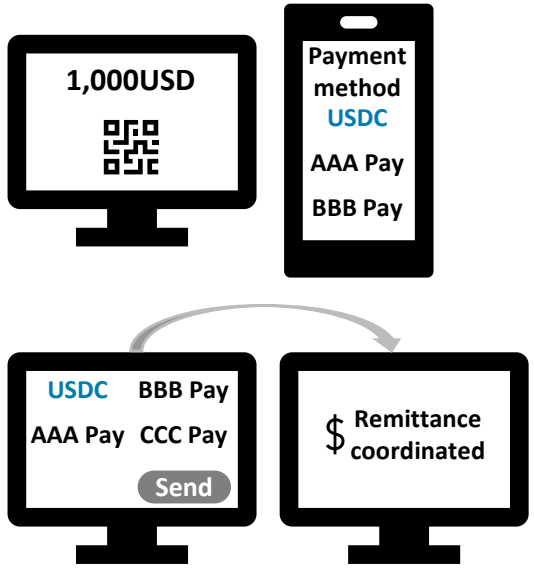
Circle's Partnerships and Investments: Partnerships with Merchant Systems

Pockyt Partners with Circle to Support Retailers Worldwide with Seamless USDC Payments

Overview

- Pockyt will be able to integrate Circle's USDC capabilities, enabling merchants to utilize stablecoins as an additional option for both deposits and payments.
- Providing merchants with a secure, efficient, and cost-effective solution for cross-border transactions using USDC.

Service Image



- USDC can be used as a payment option when accepting payments from users.
- USDC can be used as a payment option when sending funds to recipients.

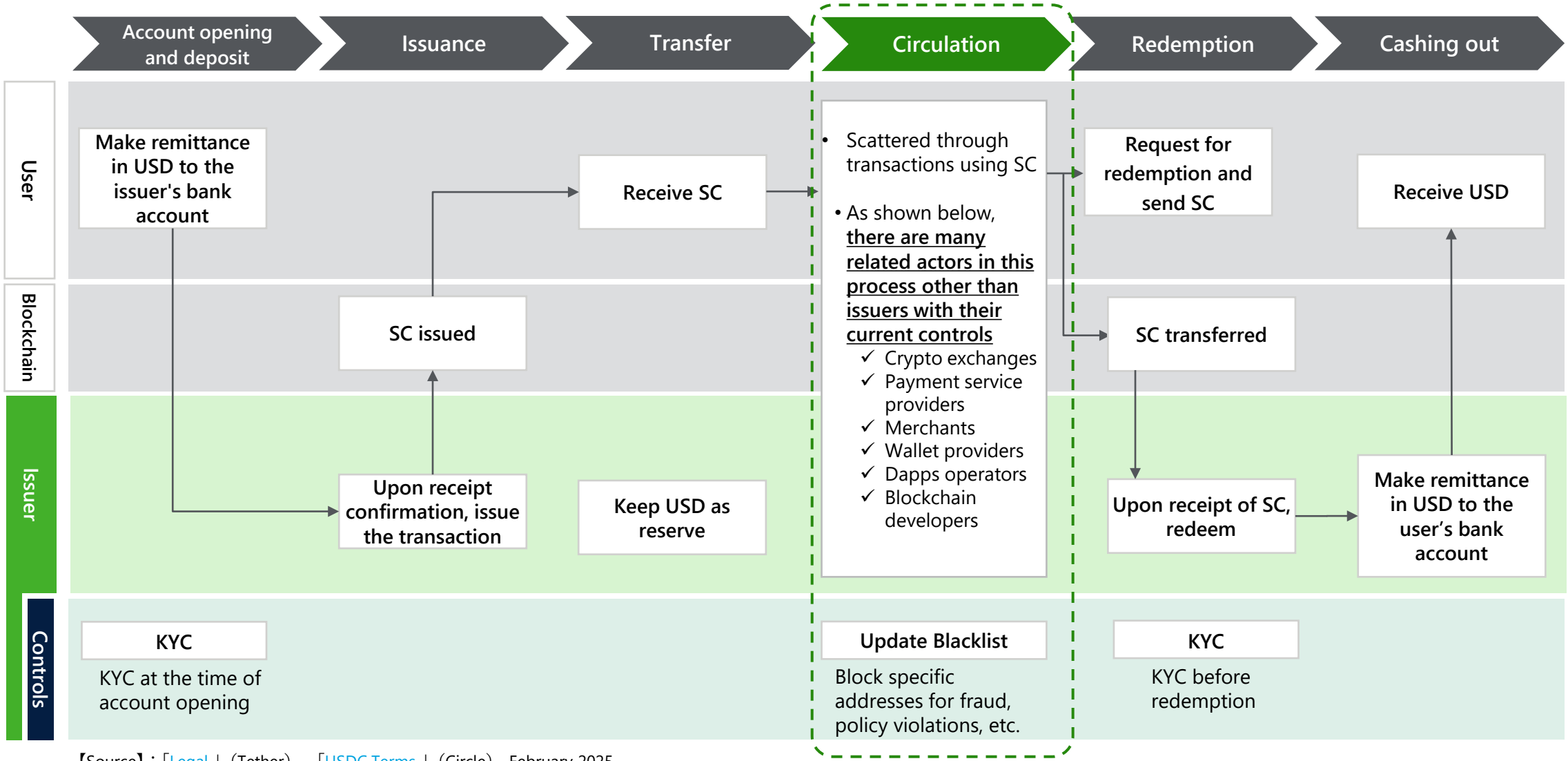
Source: Based on "News Release | Orient Corporation (Orico)" and "Pressroom | Latest Circle News (Circle)", created by our company, confirmed as of February 2025.

3. Research on Major Stablecoin Issuers

3.3 Issuance/Redemption in Smart Contract

Stablecoin’s lifecycle from issuance to redemption

Issuers have implemented controls to prevent illicit use of stablecoins, such as KYC for issuance and redemption and Blacklist to block illicit addresses or freeze funds. However, these controls have limited effect within certain processes.



【Source】:「Legal」（Tether）、「USDC Terms」（Circle）_February 2025

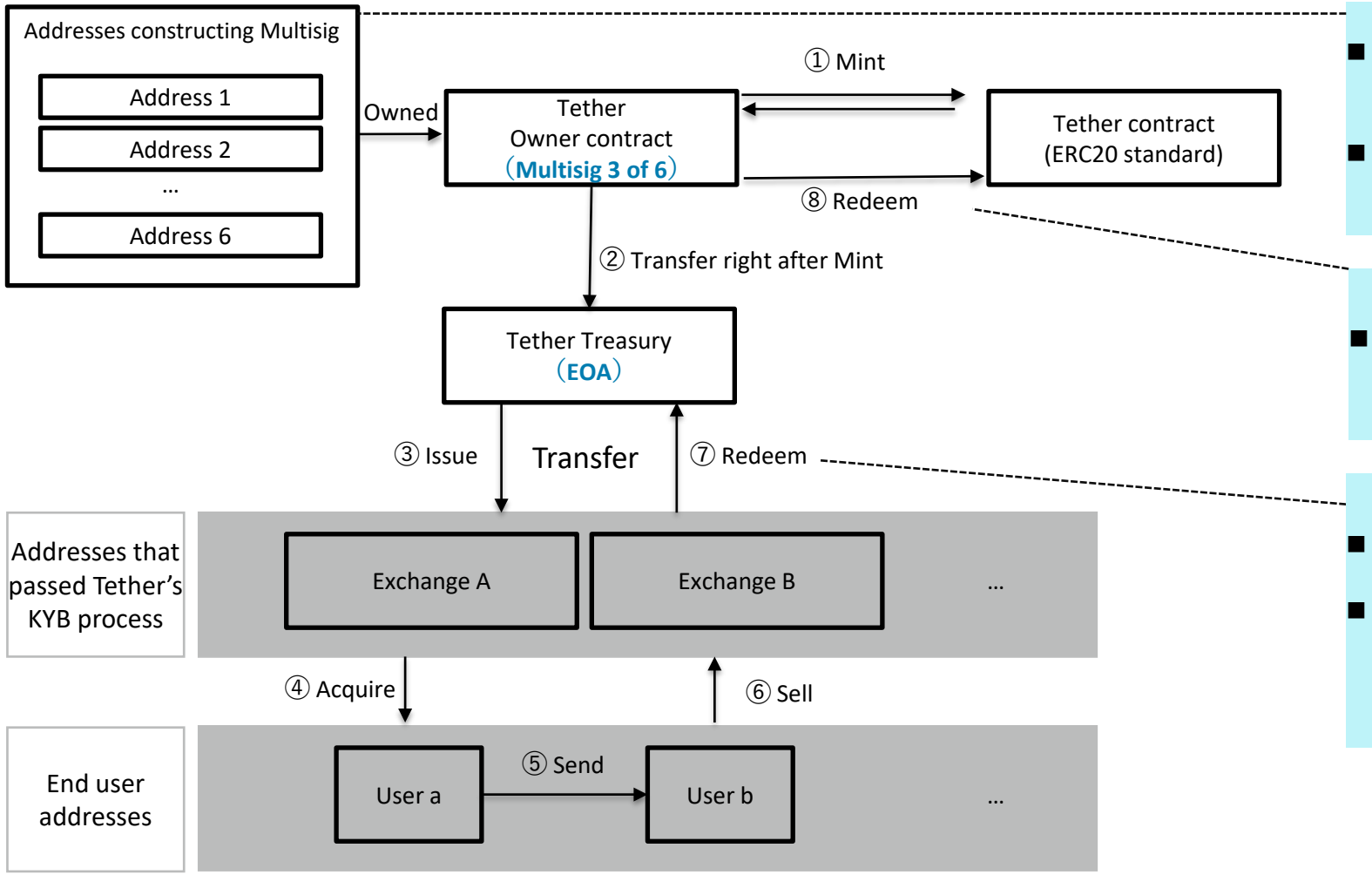
Common functions of USDT/USDC contracts

There is no significant difference in basic functions between USDT and USDC contracts, including Mint/Burn functions and Blacklisting function to block illicit uses or policy violations.

#	Functions	USDT (Tether)	USDC (USD Coin)
1	**ERC-20 Standard Functions**	All ERC-20 standard functions are implemented: name(), symbol(), decimals(), totalSupply(), balanceOf(address), transfer(address,uint256), transferFrom(address,address,uint256), approve(address,uint256), allowance(address,address)	Same as USDT
2	**Mint/Burn**	**Only Owners** can use these functions: - issue(uint256): function to mint coins - redeem(uint256): function to burn coins. Owners only.	Only Minters can use these functions: - mint(address,uint256): function to mint coins - burn(uint256): function to burn coins
3	**Minter Settings**	No Minter settings (for only Owners can mint/burn coins)	**MasterMinter can set new Minters and their upper limits of issuance** - configureMinter(address minter, uint256 minterAllowedAmount) - updateMinterAllowance(address minter, uint256 amount)
4	**Blacklisting**	**Only Owners** can use these functions: - addBlackList(address _evilUser) - removeBlackList(address _clearedUser) - **destroyBlackFunds(address _blackListedUser) :function to seize illicit funds**	Only Blacklisters can use these functions: - blacklist(address _account) - unBlacklist(address _account)
5	**Pause/Unpause**	**Only Owners** can use these functions: - pause() - unpause()	Only Pausers can use these functions: - pause() - unpause()

USDT’s issuance/redemption process from address perspective

Issuance and redemption of USDT is aggregated under Owner contract and Multisig managed.



- The Owner account consists of 3 out of 6 Multisig addresses, so only three signatures are required to Mint and Redeem.
- The Owner account has high permissions such as Blacklisting.

- Redeem at this level rarely happens (Ethereum has only had three cases in history)

- Transfers from/to Tether Treasury are defined as ‘issuance/redemption’.
- These transfers are different from Mint or Redeem on the blockchain but fall under the category of Transfer transactions.

Explanation of USDT contract - Issuance/Redemption

In USDT contract, the design is relatively simple that, only Owner account can execute Issuance and Redemption.

(Codes from USDT contract)

```
402     // Issue a new amount of tokens
403     // these tokens are deposited into the owner address
404     //
405     // @param _amount Number of tokens to be issued
406     function issue(uint amount) public onlyOwner {
407         require(_totalSupply + amount > _totalSupply);
408         require(balances[owner] + amount > balances[owner]);
409
410         balances[owner] += amount;
411         _totalSupply += amount;
412         Issue(amount);
413     }
414
415     // Redeem tokens.
416     // These tokens are withdrawn from the owner address
417     // if the balance must be enough to cover the redeem
418     // or the call will fail.
419     // @param _amount Number of tokens to be issued
420     function redeem(uint amount) public onlyOwner {
421         require(_totalSupply >= amount);
422         require(balances[owner] >= amount);
423
424         _totalSupply -= amount;
425         balances[owner] -= amount;
426         Redeem(amount);
427     }
```

Issue: Owner issues a certain amount of tokens and adds the same amount to Owner's balance.

406	Restrict function execution permission to the Owner (onlyOwner)
407	Check the supply total (Whether it overflows when the issue amount is added to the current supply total)
408	Check the Owner's balance (Whether it overflows when the issue amount is added to the current balance)
410	Add the issue amount to Owner's balance
411	Add the issue amount to the supply total
412	Log the issue amount (Event log the issue amount to blockchain)

Redeem: Owner redeems a certain amount of tokens and reduces the same amount from Owner's balance.

420	Restrict function execution permission to the Owner (onlyOwner)
407	Check the supply total (To ensure that the current supply total is equal to or greater than the redeem amount)
408	Check the Owner's balance (To ensure that the current balance is equal to or greater than the redeem amount)
410	Reduce the redeem amount from supply total
411	Reduce the redeem amount from Owner's balance
412	Log the redeem amount (Event log the redeem amount to blockchain)

Explanation of USDC contract - Issuance

In USDC contract, the issuance process is more detailly designed, including screening the Blacklist.

(Codes from USDC contract)

```
114     /**
115      * @notice Mints fiat tokens to an address.
116      * @param _to The address that will receive the minted tokens.
117      * @param _amount The amount of tokens to mint. Must be less than or equal
118      * to the minterAllowance of the caller.
119      * @return True if the operation was successful.
120      */
121     function mint(address _to, uint256 _amount)
122         external
123         whenNotPaused
124         onlyMinters
125         notBlacklisted(msg.sender)
126         notBlacklisted(_to)
127         returns (bool)
128     {
129         require(_to != address(0), "FiatToken: mint to the zero address");
130         require(_amount > 0, "FiatToken: mint amount not greater than 0");
131
132         uint256 mintingAllowedAmount = minterAllowed[msg.sender];
133         require(
134             _amount <= mintingAllowedAmount,
135             "FiatToken: mint amount exceeds minterAllowance"
136         );
137
138         totalSupply_ = totalSupply_.add(_amount);
139         _setBalance(_to, _balanceOf(_to).add(_amount));
140         minterAllowed[msg.sender] = mintingAllowedAmount.sub(_amount);
141         emit Mint(msg.sender, _to, _amount);
142         emit Transfer(address(0), _to, _amount);
143         return true;
144     }
```

Mint: Minter, authorized by Owner, mints a certain amount of tokens to an address.

121-127	Conditions/Requirements for the Mint whenNotPaused：The contract status is not Paused onlyMinters：This is a Minter's address notBlacklisted(msg.sender)：The caller is not on the Blacklist notBlacklisted(_to)：The mint to address is not on the Blacklist
129	Check the mint to address (To ensure that it is not a zero address)
130	Check the mint amount (To ensure that it is greater than zero)
132	Get the Minter's current upper limit to mint
133-135	Check the mint allowance (To ensure that the Minter does not mint over the set limit)
138	Add the mint amount to the supply total
139	Add the mint amount to the mint to address
140	Reduce the mint amount from Minter's current upper limit
141	Log the mint amount (Event log the Minter, the mint to address and the mint amount to blockchain)
142	Log the transfer amount (Event log the zero address, the mint to address and the mint amount to blockchain)

Explanation of USDC contract - Redemption

In USDC contract, the redemption process is more detailly designed, including screening the Blacklist.

(Codes from USDC contract)

```
354     /**
355      * @notice Allows a minter to burn some of its own tokens.
356      * @dev The caller must be a minter, must not be blacklisted, and the amount to burn
357      * should be less than or equal to the account's balance.
358      * @param _amount the amount of tokens to be burned.
359      */
360     function burn(uint256 _amount)
361         external
362         whenNotPaused
363         onlyMinters
364         notBlacklisted(msg.sender)
365     {
366         uint256 balance = _balanceOf(msg.sender);
367         require(_amount > 0, "FiatToken: burn amount not greater than 0");
368         require(balance >= _amount, "FiatToken: burn amount exceeds balance");
369
370         totalSupply_ = totalSupply_.sub(_amount);
371         _setBalance(msg.sender, balance.sub(_amount));
372         emit Burn(msg.sender, _amount);
373         emit Transfer(msg.sender, address(0), _amount);
374     }
```

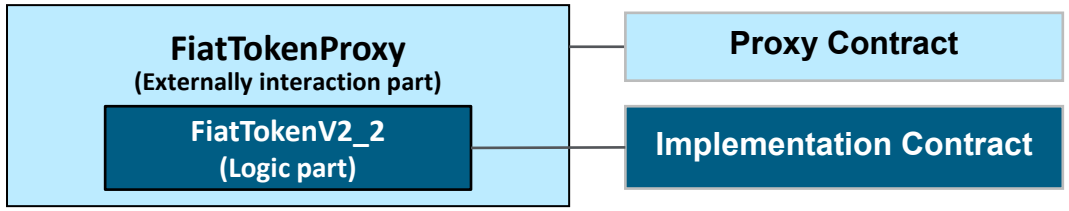
Burn: Minter, authorized by Owner, burns a certain amount of tokens from an address.

360-364	Conditions/Requirements for the Burn whenNotPaused：The contract status is not Paused onlyMinters：This is a Minter's address notBlacklisted(msg.sender)：The caller is not on the Blacklist
366	Get the caller's balance
367	Check the burn amount (To ensure that it is greater than zero)
368	Check the caller's balance (To ensure that the burn amount does not exceed the current balance)
370	Reduce the burn amount from the supply total
371	Reduce the burn amount from the caller's balance
372	Log the burn amount (Event log the caller and the burn amount to blockchain)
373	Log the transfer amount (Event log the caller, the zero address and the burn amount to blockchain)

Implementation of USDC smart contract

Since USDC is implemented using Proxy Contract, it is flexible to update the smart contract, and the role settings of the contact is designed relatively detailed.

■ USDC smart contract is implemented with **two tiers: the Proxy Contract and the Implementation Contract**, which is different from USDT implemented as an Implementation Contract.



■ Functions in FiatTokenV2_2

Function	Description
Regular ERC20	Regular ERC20 functions (Mint,Transfer,Burn)
Pause	Pauser can pause the entire contract in the case of emergency
Blacklisting	Blacklist certain addresses to prevent funds from being transferred

■ USDC has layered role settings, which is different from USDT which has only one Owner.

Role	Description
Owner	The contract Owner who can make change to MasterMinter
MasterMinter	• Can add new Minters and set Minters' upper limit to mint • Can remove existing Minter
Minter	Can Mint/Burn tokens
Pauser	can pause the whole contract in the case of emergency
Blacklister	Can Blacklist certain addresses or remove certain addresses from the Blacklist

■ There are several Minters accounts shown as below, and a control of upper limit that each Minter is allowed to mint is applied, but with current setting of these limits, only few accounts can actually mint.

#	Minter's address (as of January 31, 2025)	Upper limit to mint
1	0x5b6122c109b78c6755486966148c1d70a50a47d7	4,006,607,385
2	0xc4922d64a24675e16e1586e3e3aa56c06fabe907	86,737,797
3	0x19a932fc5a8320939c3575302a8705147a7f27d8	23,695
4	0x911cb2323c6fb580e39f92a6f58d1cb019e940cd	0
5	0x895f07957b863f4ab6086035a6990d8366bc3266	0
6	0x2322e81db282f22849c2eb0b749c688ea3611946	0
7	0x24bdd8771b08c2ea6fe0e898126e65bd49021be3	0
8	0x55fe002aeff02f77364de339a1292923a15844b8	0
9	0x3005a4c0efe7e66f3f60ef8704983247a5c6ca61	0
10	0x8967a7ce20043f876e42f8ad696b06bb632f0ca7	0
11	0x2b52e60c844d7946b6d910d3296940dc889cc785	0
12	0xe400d09e98a5806bf501e93ed8e7623b78b4646f	0
13	0x9c08210cc65b5c9f1961cdbd9ea9bf017522464d	Disabled *
14	0xd4c1315948125cd20c11c5e9565a3632c1710055	Disabled *
15	0xe7ab0dd2a069fa115c0d7878af6fd95ba0f9100a	Disabled *

*Once was a Minter but is currently disabled

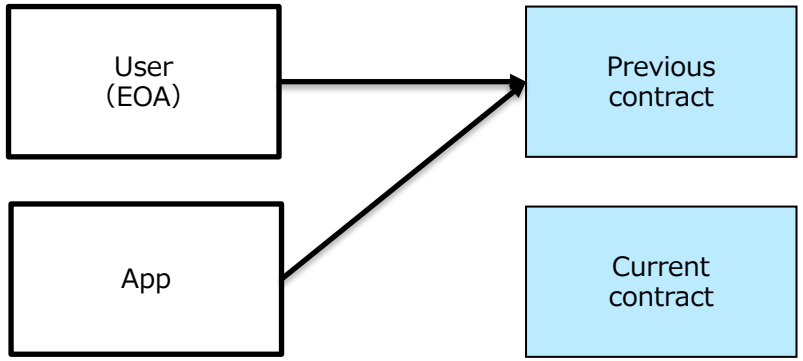
Proxy contract

Proxy Contracts are often used to make smart contract updates easier.

- There are two types of smart contracts: the Proxy Contracts and the Implementation Contracts. Their roles are summarized below.

Challenges

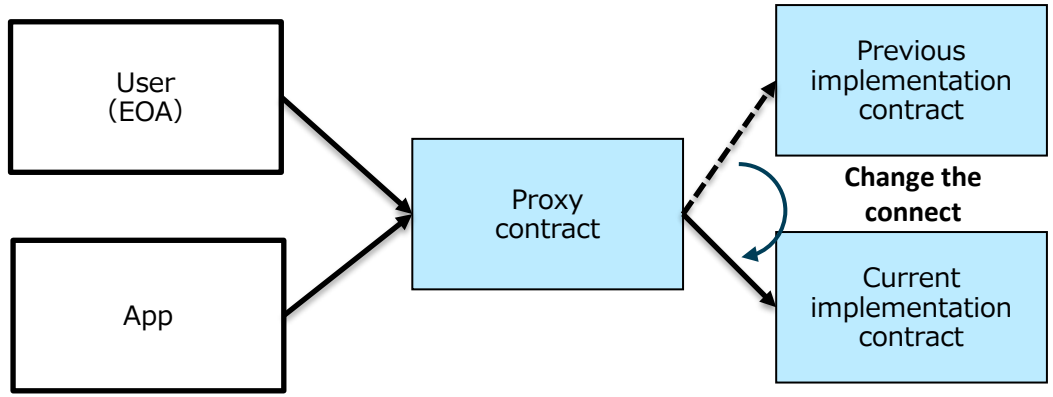
- When a smart contract is deployed, a contract address is automatically issued.
- Therefore, if new features are launched or vulnerabilities are discovered, the smart contract will be redeployed with a new contract address, the change in the address that serves as the point of contact for users and applications makes it difficult to update contracts.



The operating entity updated the contract, but users and applications remained connected to the previous contract cannot benefit from the update.

Solutions

- For important smart contracts that require maintenance, a Proxy Contract functions as the point of contact for users and applications, while the actual contract logic is contained in a separate Implementation Contract. This two-tier structure can well support upgrades.



[Reference] Basic functions from USDT smart contract

Descriptions and permission settings of basic functions from USDT smart contract

#	Function	Description	Roles with permissions	Other conditions/requirements
1	**issue(uint amount)**	Issue new tokens and add the amounts to the Owner's balance	**onlyOwner**	-
2	**redeem(uint amount)**	Redeem tokens from the total supply and reduce the amounts from the Owner's balance	**onlyOwner**	-
3	**addBlackList (address _evilUser)**	Blacklist certain addresses to prevent fund transfer Inside the function set 'isBlackListed[_evilUser] = true'	**onlyOwner**	-
4	**removeBlackList(address _clearedUser)**	Remove certain addresses from the Blacklist Inside the function set 'isBlackListed[_clearedUser] = false'	**onlyOwner**	-
5	**destroyBlackFunds(address _blackListedUser)**	Seize/Burn the tokens belong to Blacklisted addresses and reduce the total supply	**onlyOwner**	The subject address is on the Blacklist
6	**pause()**	Pause the contract in the case of illicit transactions or emergencies	**onlyOwner**	The contract is not yet in the paused status (paused == false)
7	**unpause()**	Reopen the contract that was paused	**onlyOwner**	The contract is in the paused status (paused == true)
8	**transfer(address _to, uint _value)**	A standard ERC20 function that transfers tokens Transfers from Blacklisted addresses will be rejected Includes the calculation of transaction fees	**All users that not on the Blacklist**	The contract is not in the paused status (paused == false) The destination address is not on the Blacklist

[Reference] Basic functions from USDC smart contract

Descriptions and permission settings of basic functions from USDC smart contract

#	Function	Description	Roles with permissions	Other conditions/requirements
1	**mint(address _to, uint256 _amount)**	Mint new tokens to an address	**Minter**	The contract is not in the paused status The mint to address is not on the Blacklist The mint amount is within the Minter's upper limit (minterAllowance)
2	**burn(uint256 _amount)**	Burn tokens and reduce the amount from the caller's balance and from the total supply	**Minter**	The contract is not in the paused status The caller is not on the Blacklist The burn amount does not exceed the caller's balance
3	**blacklist(address _account)**	Blacklist certain addresses and prohibit transfer, issuance and redemption from those addresses	**Blacklister**	The subject address is not address(0)
4	**unBlacklist(address _account)**	Remove certain addresses from the Blacklist and remove restrictions on them	**Blacklister**	The subject address is on the Blacklist
5	**pause()**	Pause the entire contract and all functions including transfer, issuance, and redemption are suspended.	**Pauser**	The contract is not yet in the paused status
6	**unpause()**	Reopen the contract and all functions such as transfer, issuance, and redemption are resumed	**Pauser**	The contract is in the paused status (paused = true)
7	**transfer(address to, uint256 value)**	A standard ERC20 function that transfers tokens from the caller address to the destination address	**All users that not on the Blacklist**	The contract is not in the paused status Both the caller and the destination address are not on the Blacklist The transfer amount does not exceed the caller's balance

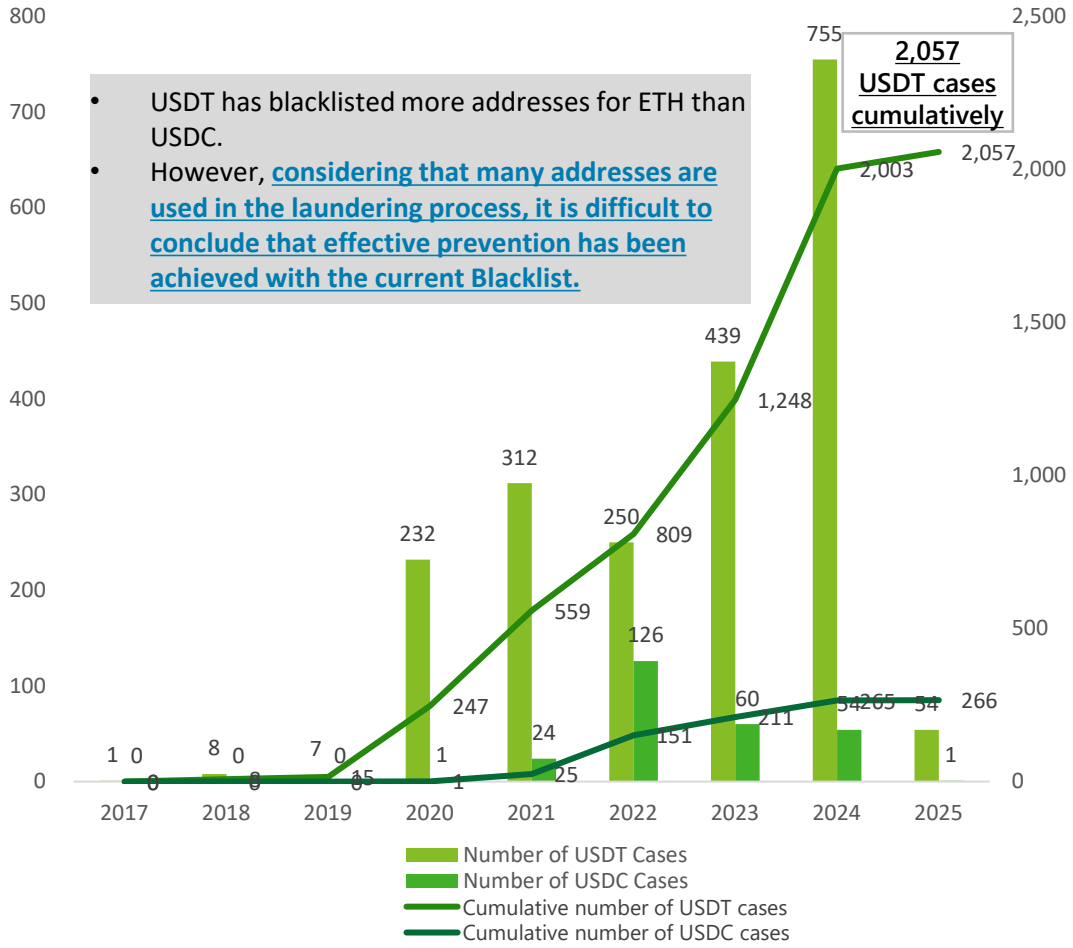
3. Research on Major Stablecoin Issuers

3.4 Blacklisting by Issuers

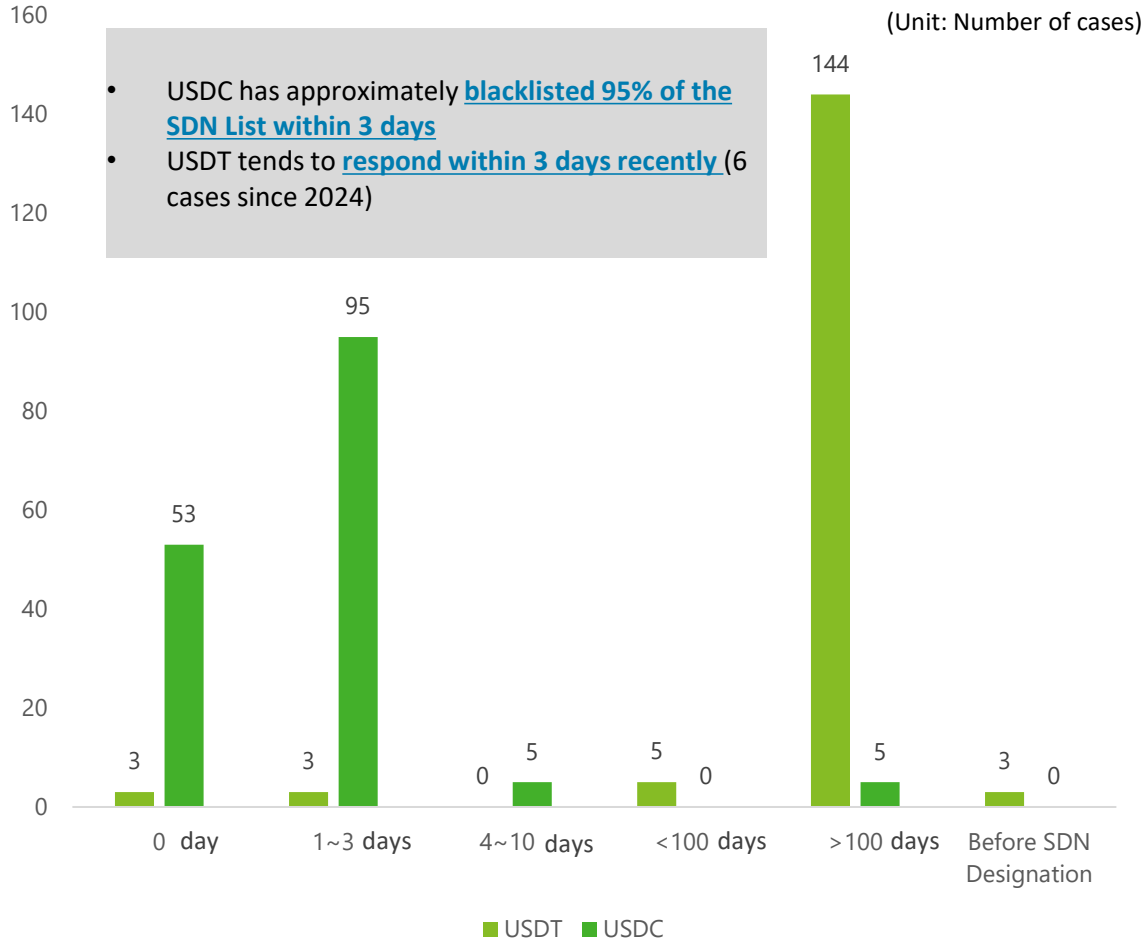
Blacklisted addresses for ETH by issuers

USDC has blacklisted fewer addresses than USDT but tends to respond quickly to sanctions.

Trend in the number of blacklist entries



Duration from SDN listing to Blacklisting



Issuer’s response to regulatory movements (USDT)

Tether has been assisting the authorities’ investigations on crypto crimes to freeze linked assets in USDT.

#	Date	Regulatory movements	Tether's response
1	October 2021	• The Commodity Futures Trading Commission (CFTC) issued an order simultaneously filing and settling charges against Tether for making untrue or misleading statements and omissions of material fact in connection with USDT. The order requires Tether to pay a civil monetary penalty of $41 million. • The CFTC also issued a separate order simultaneously filing and settling charges against Bitfinex requiring a $1.5 million civil monetary penalty.	• Tether paid the fine and agreed to respond to violations of the Commodity Exchange Act (CEA) and CFTC regulations.
2	November 2023	• United States Department of Justice (DOJ) ,with assistance from Tether and OKX, investigated an international human trafficking syndicate in Southeast Asia responsible for a global “pig butchering” romance scam, that led to the freezing of approximately 225 million in USDT tokens in external self-custodied wallets linked to it.	• Tether proactively and voluntarily froze approximately 225 million in USDT tokens related to the criminal organization. • During a months-long investigative effort by Tether and OKX, U.S. law enforcement agencies, including the DOJ, were proactively alerted to the location of the illicit funds by analyzing the flow of those funds through the blockchain. • To the extent lawful wallets were captured by this operation, Tether stated that it will work quickly with law enforcement and the owners of those wallets to unfreeze them, as appropriate.
3	September 2024	• U.S. Department of Justice (DOJ) seized over $6 million in assets linked to a crypto-confidence scheme based in Southeast Asia.	• Tether assisted the DOJ in seizing over $6 million in assets linked to the crypto-confidence scheme.

【Source】：「CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million」（CFTC）「Tether News」（Tether, November 2023 and September 2024）_January 2025

Issuer’s response to regulatory movements (USDC)

Circle has responded to requests from authorities by blocking services subject to OFAC sanctions.

#	Date	Regulatory movements	Circle's response
1	August 2022	The U.S. Department of the Treasury’s (Treasury) Office of Foreign Assets Control (OFAC) added Ethereum addresses related to mixing protocol Tornado Cash to its list of sanctioned entities. • In OFAC’s press release, they stated that Tornado Cash has been used to launder more than $7 billion worth of virtual currency in the past 3 years. *1	• On August 9, Circle blocked 38 addresses associated with Tornado Cash. • Circle also announced to restrict USDC movement related to Tornado Cash addresses. • Under the Bank Secrecy Act (BSA), Circle is required to block transactions with sanctioned addresses.
2	May 2023	The OFAC settled with Poloniex, LLC, a Circle subsidiary, for $7,591,630 related to apparent violations of multiple sanctions programs.	Circle implemented its own compliance measures for the Poloniex Trading Platform, which further improved Poloniex’s sanctions compliance program. Those measures, in addition to other subsequent remedial measures, included: • Freezing users’ accounts until KYC verification was completed; • Implementing an automated review and verification tool for identity documents; • Implementing a protocol that prevented users from activating an account if the profile information matched a sanctioned country; • Implementing geolocation restrictions with respect to Syria, Iran, Cuba, Sudan, and North Korea; • Closing any accounts that listed “Crimea” in the profile information, and identification and blocking of IP ranges associated with certain internet service providers operating in Crimea; • Creating a “Crimea IP blacklist” and “Crimean city/region keywords list” against which all account information was screened; and • Enhancing its training program and hiring additional experienced compliance personnel.

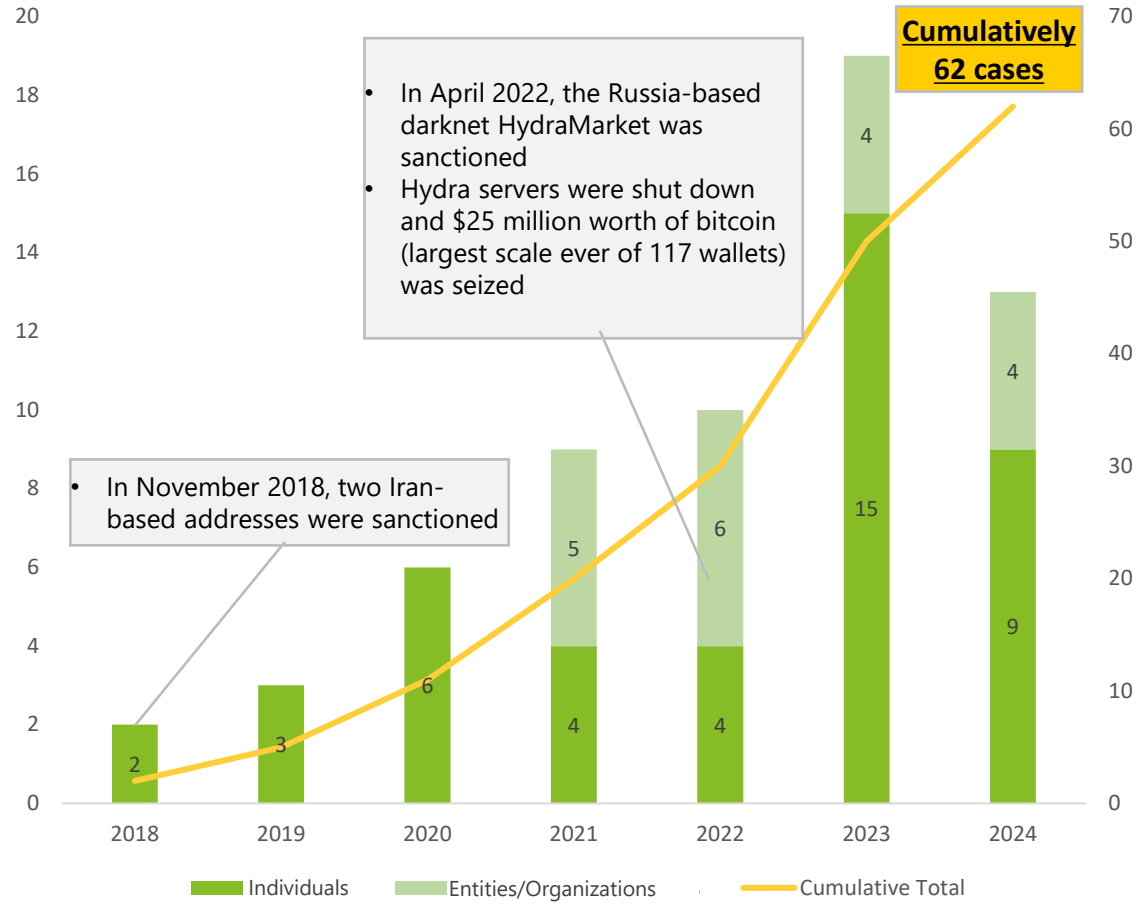
【Source】：「OFAC Sanctions Tornado Cash: Issues & Implications」（Galaxy）「A Settles with Poloniex, LLC for $7,591,630 Related to Apparent Violations of Multiple Sanctions Programs」（OFAC）_February 2025

*1 The U.S. Department of the Treasury lifted sanctions on Tornado Cash on March 21.「Tornado Cash Delisting」（U.S. Treasury）

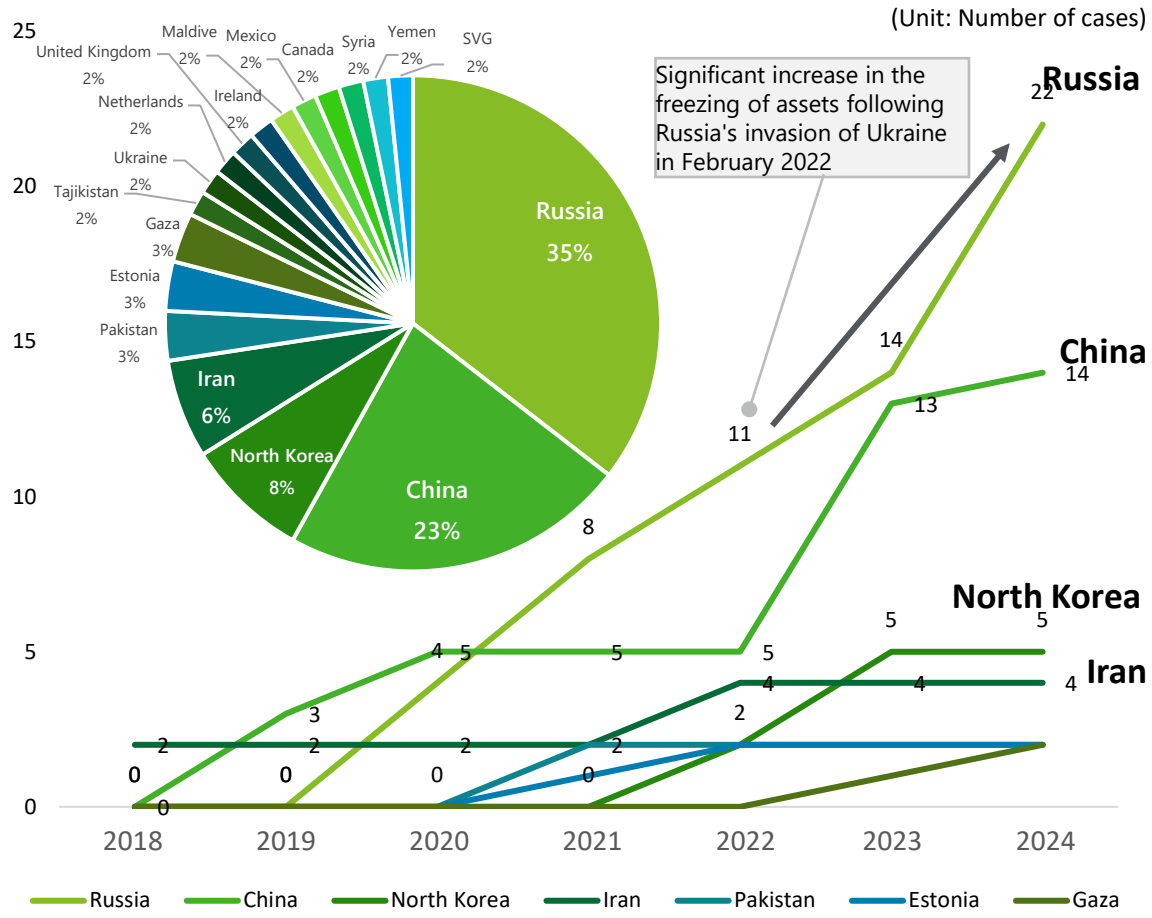
Trend of OFAC's SDN listing

The SND listing of crypto addresses began in November 2018, and out of the total SDN list of approximately 17,000 cases, 62 cases are related to crypto assets as of the end of 2024.

Trend in number of SDN listing of crypto addresses



Cumulative crypto address SDN list by country



【Source】「OFAC SDN LIST」（OFAC）_January 2025, OFAC Press Releases（OFAC）_November 2018,「OFAC Press Releases」（OFAC）_April 2022

Number of OFAC's SDN listed crypto related cases (by Sanctions Program)

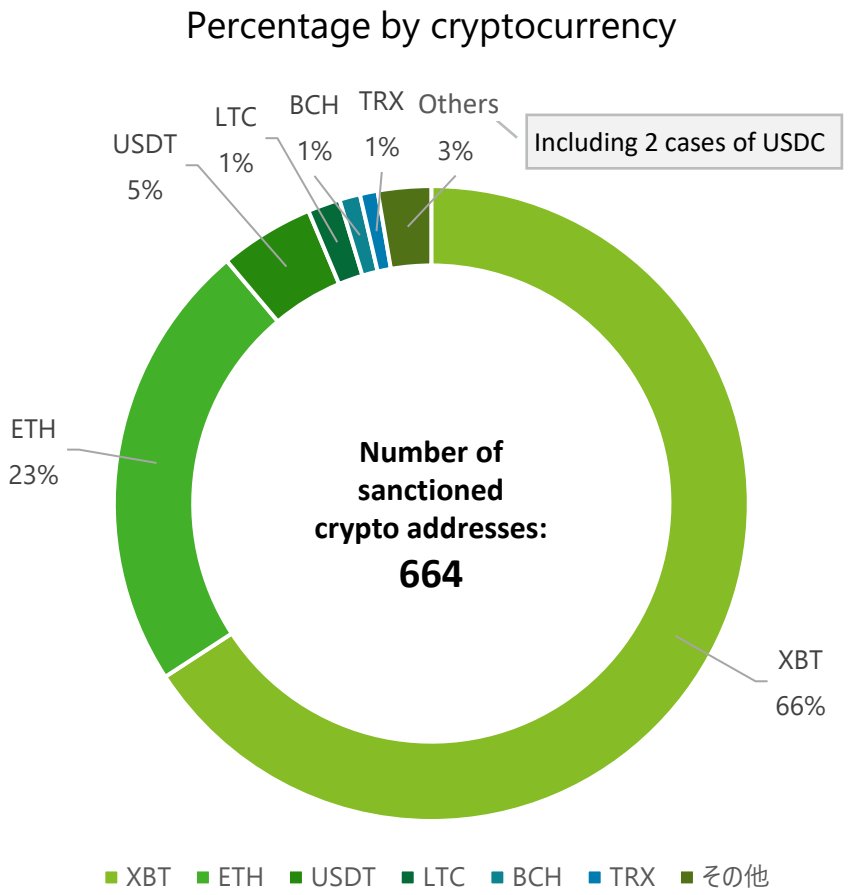
The sanctioned crypto addresses are listed most for the reason of cyber attacks, followed by drug trafficking, Russia, and North Korea.

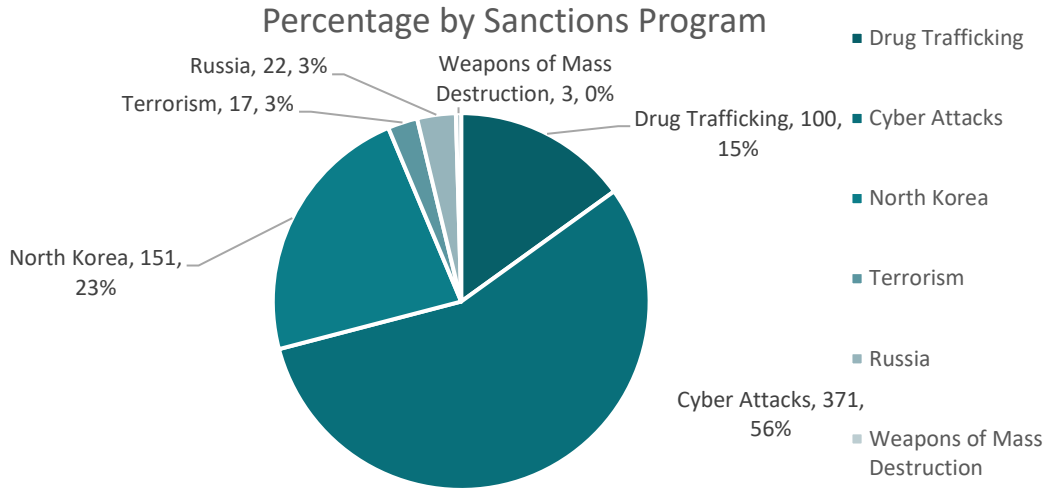
Category	Program tag	Number of cases (by category)	Number of cases (by program)	Definition
Cyber Attacks	CYBER2	23 (37%)	14	Sanctions Against Individuals Involved in Cyber Attacks
	CYBER2/ELECTION-EO13848		4	Sanctions Related to Cyber Attacks and Election Interference
	CYBER2/RUSSIA-EO14024		1	Sanctions Related to Cyber Attacks and Russia's Malicious Activities
	IRGC/IFSR/CYBER2		2	Sanctions on Iran Related to Cyber Attacks
	UKRAINE-EO13661/CYBER2/ELECTION-EO13848		1	Sanctions on Ukraine Related to Cyber Attacks and Election Interference
	NPWMD/CYBER2/ELECTION-EO13848		1	Sanctions to Prevent WMD Proliferation, Cyber Attacks, and Election Interference
Terrorism	SDGT	6 (9%)	5	Sanctions Against Specific International Terrorists
	SDGT/IFSR		1	Sanctions on Specific International Terrorists and Iran
Drug Trafficking	SDNTK	14 (22%)	3	Sanctions Against Foreign Nationals and Entities Involved in Drug Trafficking
	ILLICIT-DRUGS-EO14059		11	Sanctions Against Individuals Involved in Illegal Drug Trafficking
Weapons of Mass Destruction	NPWMD	1 (1%)	1	Sanctions Related to WMD Proliferation
North Korea	DPRK4	8 (12%)	1	Sanctions Related to North Korea
	DPRK3		2	Sanctions Related to North Korea
	DPRK3/CYBER2		5	Sanctions Related to North Korea and Cyber Attacks
Russia	RUSSIA-EO14024	10 (16%)	10	Sanctions Against Individuals Involved in Russia's Malicious Activities
Total:		62		

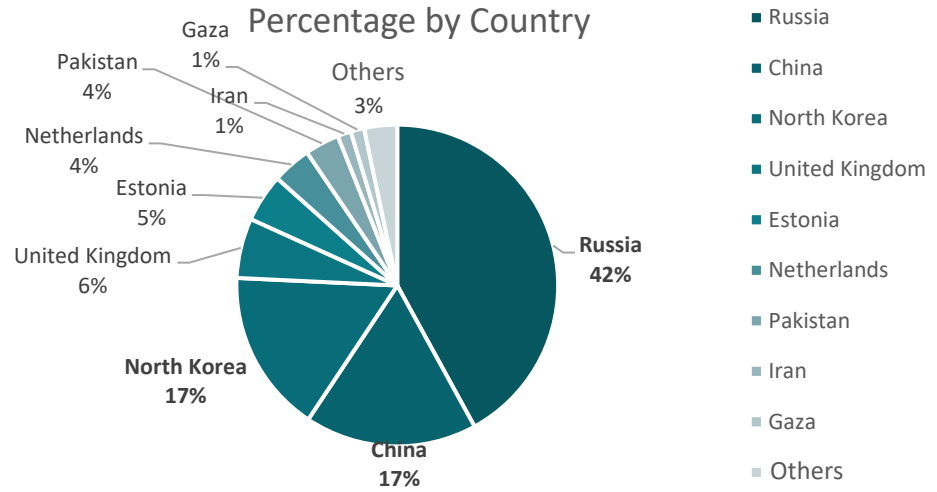
【Source】:「OFAC SDN LIST」,「Program Tag Definitions for OFAC Sanctions Lists」(OFAC, As of January 17, 2025) _January 2025

Breakdowns of OFAC's SDN listed crypto addresses

XBT (Bitcoin) and ETH account for 89% of SDN listed addresses. Out of the total number of sanctioned addresses, drug trafficking is the most listed program, and Russia the most listed country.







【Source】:「OFAC SDN LIST」(OFAC) _January 2025 Subject to individuals and organizations whose Digital Currency Address is registered.
Categorization by country is based on nationality/citizenship in the case of individuals, address, program, etc. in the case of entities/organizations.

3. Research on Major Stablecoin Issuers

3.5 Technological Trends and Issuers' New Approaches

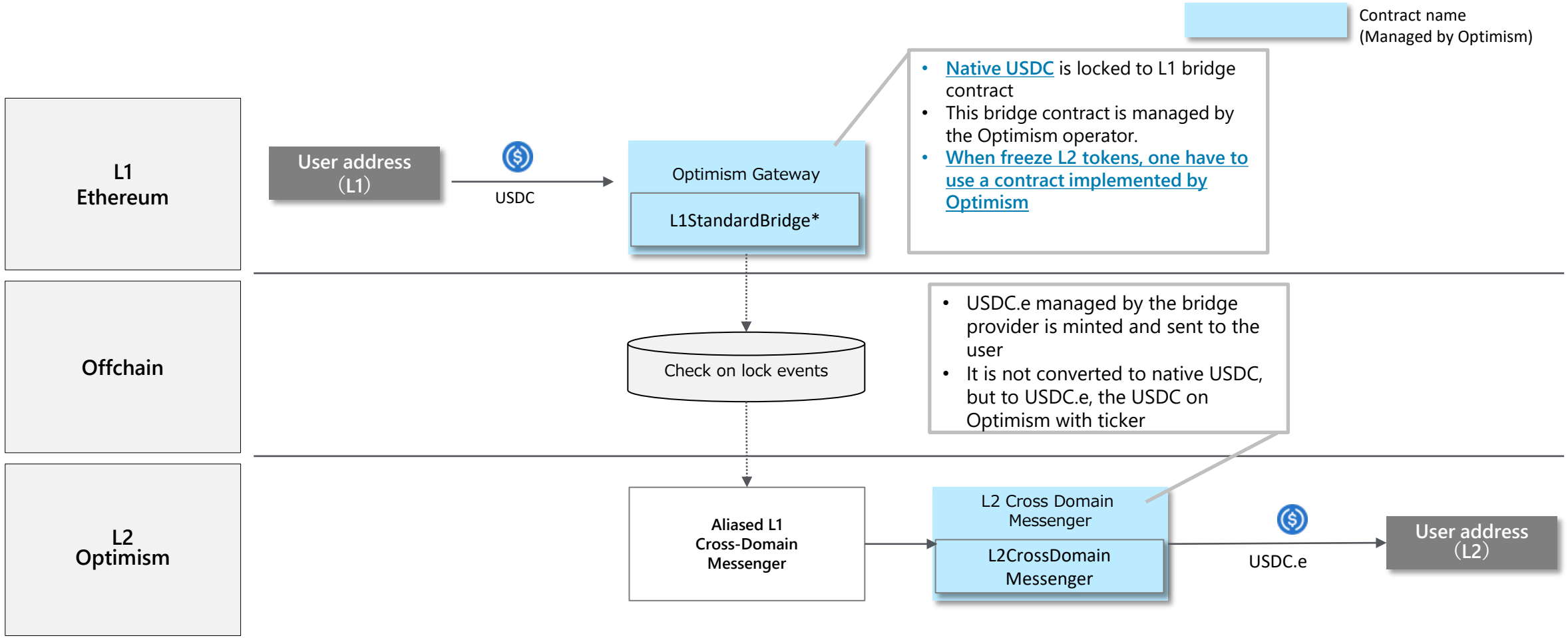
(Repost) Technologies used in laundering crypto-assets and approaches to address them

The technologies used in laundering crypto-assets include Mixing, which conceals the route of fund transfers, and Chain-hopping, which involves multiple chains. The industry-wide collaboration to track and prevent illicit use is essential nonetheless a challenge.

#	Technologies used illicitly	Approaches to address the problem	Challenges	Related protocols
①	■ **Mixing, which conceals the route of fund transfers** ➢ Conceal route of fund transfers by mixing transactions of multiple users, withdrawing to different addresses, and moving to different accounts or chains	■ **Sanction the addresses and smart contracts of mixing service providers and check the sanction list at the time of transaction** 【Countermeasures by actor】 • Issuers: Implement monitoring, tracking, and censorship functions, Restrict the use of mixing services • Service providers/Users: Check suspicious counterparties and sanction lists provided by analysis tool vendors, send alerts to users in wallets	■ How to ensure implementation of screening suspicious counterparties and sanction lists ■ How to analyze and distinguish illicit transactions from regular transactions with advanced techniques (e.g., Coinjoin)	• Centralized mixers (e.g., Blender.io) • Decentralized mixers (e.g., Coinjoin) • Smart contract-based mixers (e.g., Tornado Cash)
②	■ **Chain-hopping, which launder stablecoins through different chains, such as Layer2** ➢ Make tracking difficult by bridging illicit funds across multiple chains in a short time, using different wallets for each chain, and eventually cashing out to fiat currency through cryptocurrency exchanges or OTC/P2P transactions ➢ Make tracking difficult by bridging illicit funds to Layer2 (L2) which is designed for scalability and fee reduction, and circulating them on L2	■ **Track cross-chain transactions using blockchain analysis tools to graphically analyze information** 【Countermeasures by actor】 • Issuers: Implement monitoring, tracking, and censorship functions with analysis tools • Service providers/Users: Monitor cross-chain transactions with advanced analysis tools and codes such as AI to detect suspicious activities (e.g., Blockaid services)	■ How to collaborate and improve analysis tools, as tracking becomes difficult when involving multiple chains and layers ■ **How to choose from multiple bridging methods, as the optimal implementation of bridge differs for each player**	• Optimistic Rollup • ZK Rollup • Wrapped Tokens • Cosmos/Polkadot • Inter-Blockchain Communication • Cross-Chain Transfer Protocol (CCTP)

Optimism standard bridge (Lock & Mint)

In the case of a lock-and-mint bridge, an issue arises that the issuer cannot use the Blacklist function implemented by the issuer, because the issuer has no permission to manage the contracts for Layer2 tokens.

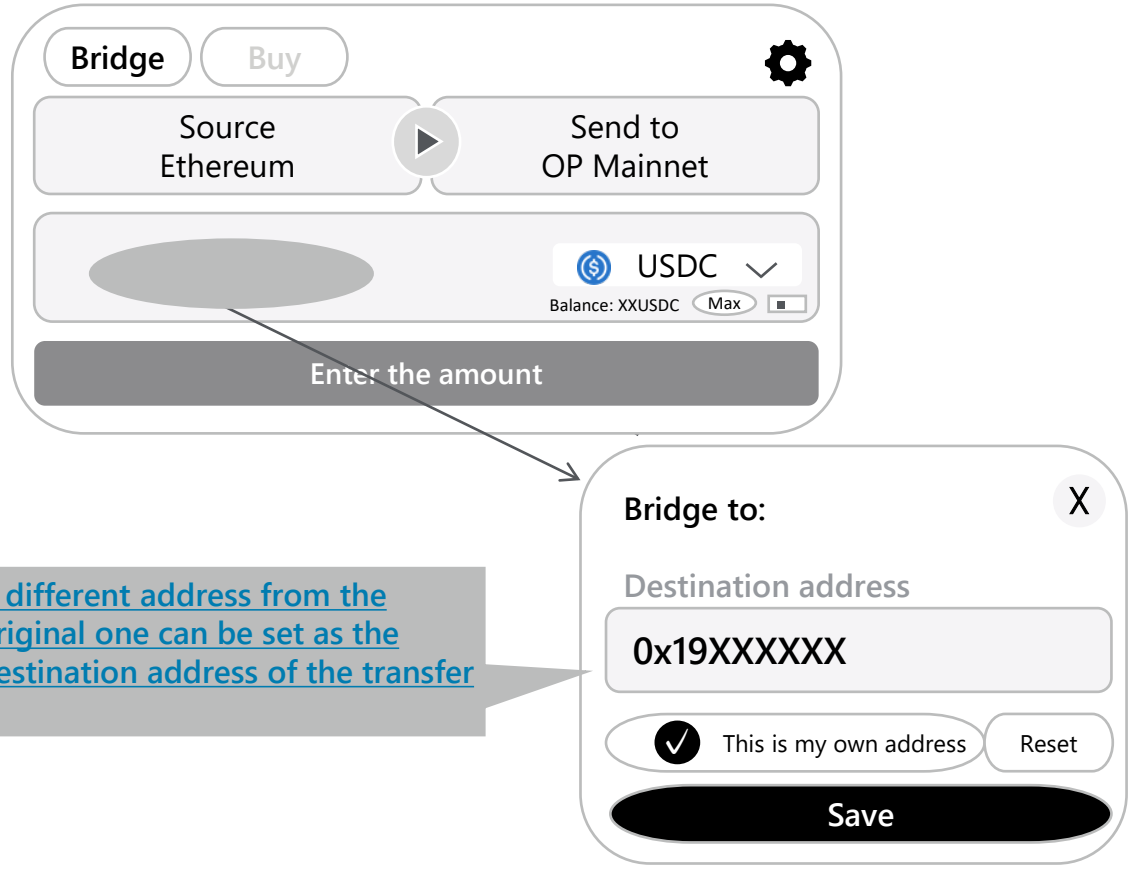


【Source】:「Transaction Details」(Etherscan) _January 2025,「Transaction Details」(Basescan) _ January 2025

Bridge's UI and Blacklist function

It is possible to implement Blacklist function in the contract of the bridge solution side, but no remarkable fact was found regarding the execution of such function.

The service, which is an aggregation of various bridges, allows users to send tokens to addresses on other blockchains, and has a user-friendly UI.



A different address from the original one can be set as the destination address of the transfer

The USDC.e contract managed by the bridge (Optimism) has Blacklist function in the source code, but there was no record of execution of Blacklisting.

1. allowance (0xdd62ed3e)
2. balanceOf (0x70a08231)
3. blacklister (0xbd102430)
   0x0000000000000000000000000000000000000000 address
4. decimals (0x313ce567)
5. isBlacklisted (0xfe575a87)
6. l1Token (0xc01e1bd6)
7. l2Bridge (0xae16faaf)
8. name (0x06fdde03)
   USD Coin *string*
9. owner (0x8da5cb5b)
   0x9028967bCb7c8eA664813714c5f2F54f84FDB308 address
10. paused (0x5c975abb)
11. pauser (0x9fd0506d)
    0x0000000000000000000000000000000000000000 address

- There is a contract named 'blacklister', but an invalid address is registered here making it no longer available.
- Further, we used Dune Analytics to investigate past events and found no record of Blacklisting any certain addresses, so the function has never been used in the past.

- The Owner is constructed from 2 of 3 Multisig by GoosisSafe, but the signature key is managed by the Optimism operator.

【Source】:「Token USD Coin (Bridged from Ethereum)」(OP Mainnet) _ January 2025

Circle CCTP (Cross-Chain Transfer Protocol)

Circle has a policy of implementing centralized management on Layer2 tokens etc. from Burn & Mint by Circle's own contracts.

Overview

■ **Overview**

- Circle CCTP (Cross-Chain Transfer Protocol) is a protocol that utilizes the burn-and-mint mechanism to enable the transfer of "always native USDC" across different blockchains.

■ **Key Features**

- Maintaining the native token nature of USDC
  USDC is issued by contracts that are entirely under Circle's control, without locking native tokens to specific contract addresses.
- Centralized management by Circle including off-chain processing
  Circle centrally manages all processes, including the oracle and verification processes, thereby preventing issues like unauthorized minting or double issuance that are concerns for other bridge solutions.
- Concerns of risk concentration at Circle
  Since Circle has an architecture that centrally manages the entirety of USDC, there is a risk of misconduct or errors by Circle itself.

Supported chanis

■ Currently supports the following 9 chains
Aribitrum, Avalanche, Base, Ethereum, Noble, OP Mainnet, PolygonPoS, Solana, Sui

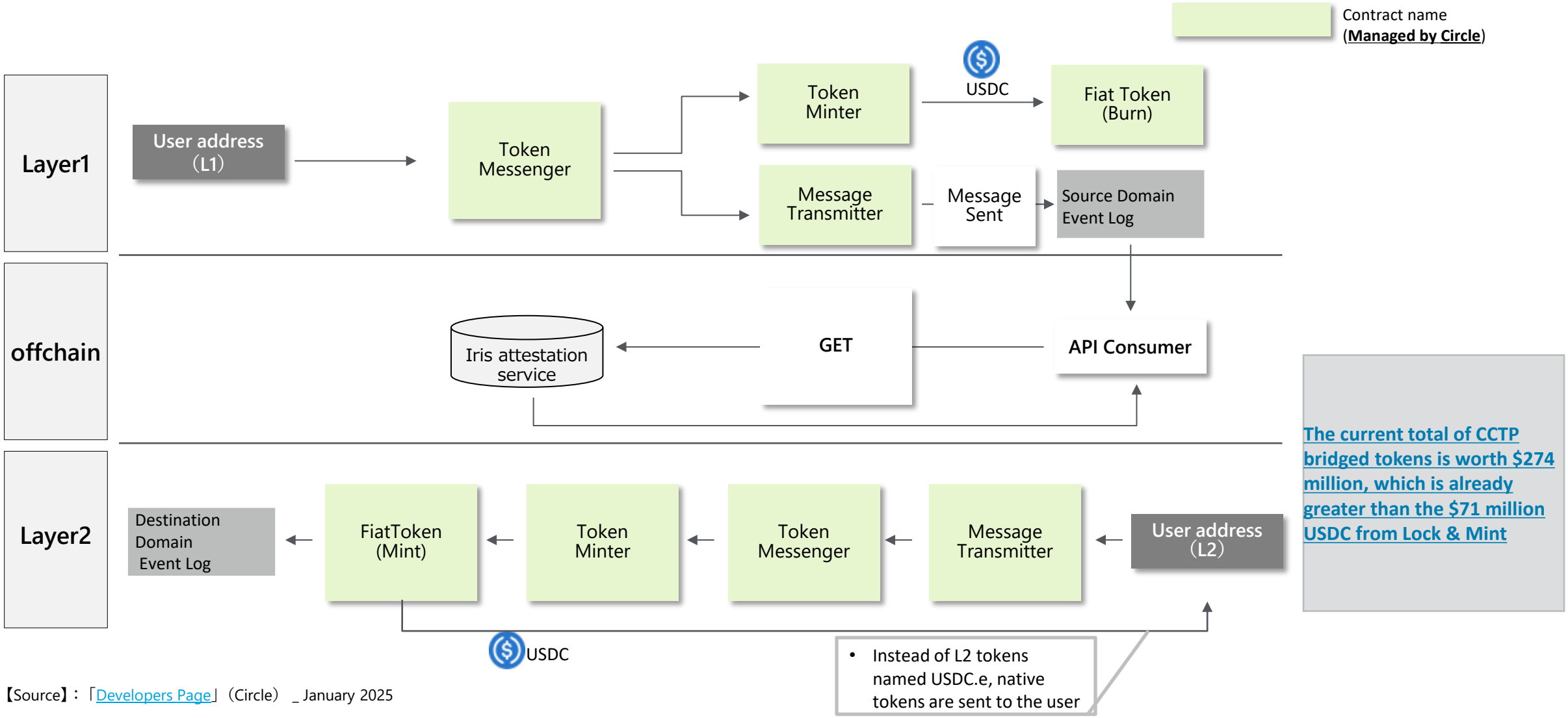
■ Will support the following chains in the near future
Aptos, Unichain

Item	Traditional bridge (Lock & Mint)	Circle CCTP（Burn & Mint）
Issuance	• Lock the tokens on the source chain to the bridge contract address, and mint the same amount of tokens on the destination chain • The bridge solution operator manages the contract	• Burn USDC on the source chain and mint USDC on the destination chain • Circle manages the contract
Redemption	• Bridged tokens are not subject to redemption directly from Circle, one needs to withdraw the tokens and return them to native tokens first and then request redemption.	• Bridged tokens can be redeemed directly from Circle, because they are Circle managed
Hacking risk	• Locking a large number of tokens on the source chain makes the contract more likely be targeted by hackers	• Low hacking risk because tokens are not locked to bridge contracts
Complexity in operations and management	• Requires trust in operators for each bridge solution • Each bridge solution has a different operating and governance model, most of which are not disclosed, lacking transparency in effectiveness assessment	• Circle's centralized management makes fraud and operational risks arising from differences in how each chain operates low
Scalability	• May require customization for each target chain	• All supported chains can be handled by a common protocol

【Source】:「cross-chain-transfer-protocol」（Circle）、「Developers Page」（Circle） _ January 2025

Circle CCTP bridge (Burn & Mint)

The burn-and-mint bridge CCTP manages issuance and redemption through the contracts implemented directly by Circle, thus enabling Blacklist function to be effective also on Layer2.



【Source】:「Developers Page」（Circle） _ January 2025

(Reference) The most recent hacking incident

The Bybit Hack - (1) How the attack occurred

In February 2025, the Bybit hack occurred and resulted in the theft of approximately $1.5 billion, which is the new record in stolen amount of a single attack.

On February 21, 2025, a theft incident occurred at the cryptocurrency exchange Bybit, where ETH worth $1.5 billion was stolen. The attack method is similar to the case of DMM Bitcoin in May 2024, which used social engineering techniques, indicating significant challenges in information sharing within the industry.

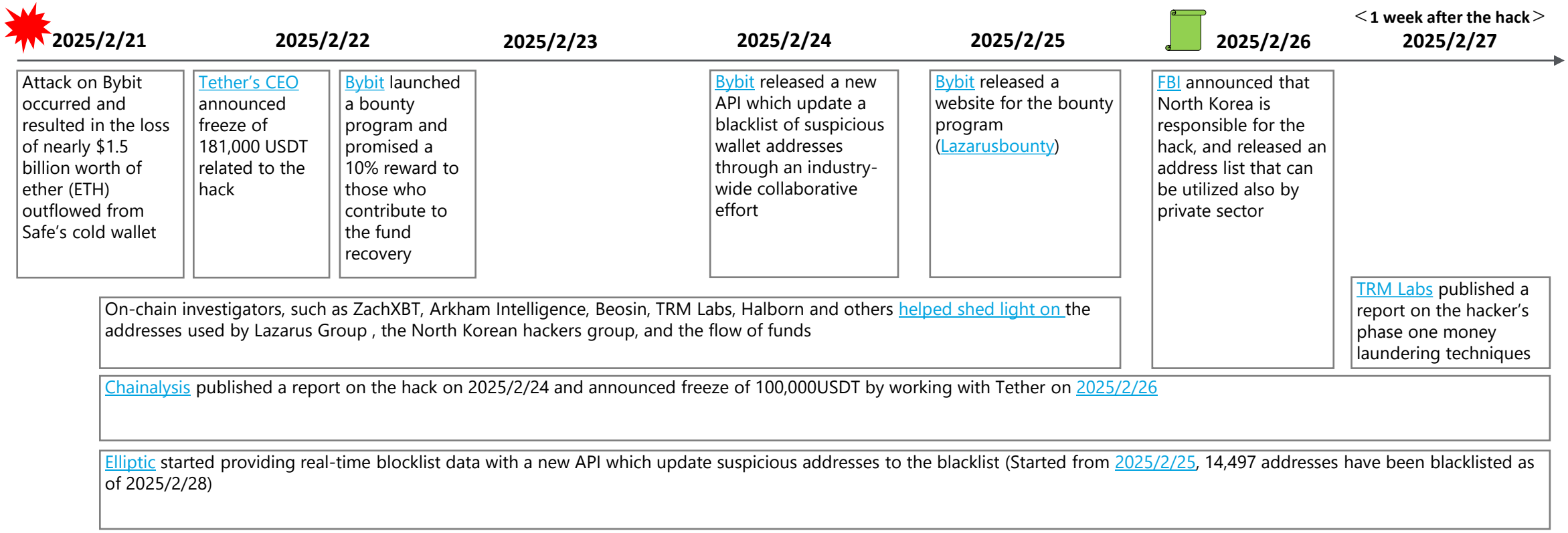
	AWS S3 script tampering	On-chain activities
Pre-event	Replace with malicious script The attacker modified front-end JavaScript files in SAFE AWS S3 buckets to embed malicious scripts. The compromised web app was provided to users and affected Bybit's signers.	Deploy rogue contracts The attacker deployed two contracts on Ethereum, a Trojan contract and a backdoor contract.
Occurrence of the event	Manipulate transactions When the signer approved the transaction in SAFE, a malicious script was run that altered the details of the transaction, such as the desitination address and the data. The information shown on the signer’s screen was correct, but the fund was actually sent to the attacker’s address. The manipulation worked only under certain conditions and did not affect ordinary users.	Direct to rogue contracts The transactions created by correct signers were executed with the Trojan contract and Bybit's cold wallet's Implementation contract was redirected to the pre-deployed backdoor contract, instead of to the normal one. Steal funds using rogue contracts The attacker used the sweepETH and sweepERC20 functions in the backdoor contract to steal ETH, stETH and other funds stored in Bybit's cold wallet.
Post-event	Destroy evidence Within two minutes of the funds being stolen, the attacker restored the JavaScript to the original one and erased the traces, thus delayed being detected.	Launder the stolen funds The attackers obfuscated the tracking of the funds by splitting them into multiple addresses or chain-hopping them to other chains.

【Source】：Illustrated by Deloitte based on public information _March 2025

The Bybit Hack - (2) Initial response to the incident

The industry actioned quickly to the incident, and within a few days they were able to identify the attacker. Through the collaborative effort, an open investigation is ongoing to track and recover the hacked funds.

After the hack occurred, there was an industry-wide collaboration involving stablecoin issuers, cryptocurrencies exchanges, on-chain investigators, analysis tool vendors, etc. and the attacker has been identified within a few days.
Bybit launched a bounty program, aiming to incentivize the crypto community to track, trace and freeze the stolen funds.



【Source】：「The Bybit Hack: Following North Korea's Largest Exploit」（TRM Labs） as of March 2025

The Bybit Hack - (3) Phase one money laundering techniques

With the hacker’s evolving laundering strategies, most of the funds have been moved and converted in a short time after the hack.

The Lazarus Group’s phase one (approximately one week) laundering process showed the following laundering strategies that make it more difficult for investigations than the group's previous hack jobs.

■ Rapid laundering

- Beyond the sheer scale of the Bybit hack, the speed at which the stolen funds are being laundered is particularly alarming.
- Within 48 hours, at least USD 160 million had been funneled through illicit channels.
- This strategy suggests that North Korea has either expanded its money laundering infrastructure or that underground financial networks, particularly in China, have enhanced their capacity to absorb and process illicit funds.

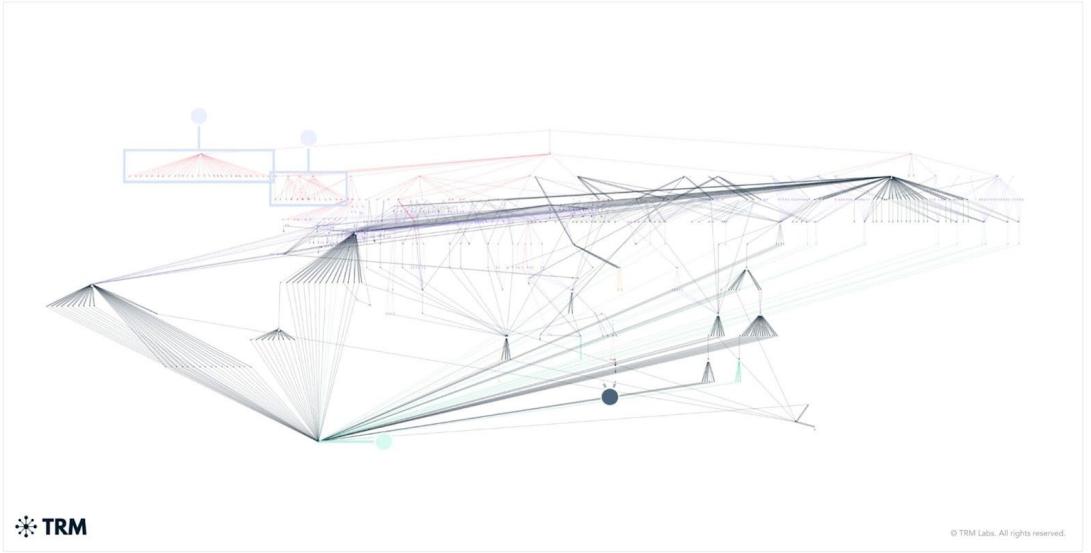
■ Multifaceted strategy

- The attackers have adopted a multifaceted strategy involving multiple intermediary wallets, decentralized exchanges, and cross-chain bridges to rapidly obfuscate the source of the funds.
- Historically, North Korean cybercriminals have relied on cryptocurrency mixers to obscure the origins of stolen funds before converting them into fiat currency. However, the vast amount of assets stolen in the Bybit attack renders traditional mixing services impractical.

■ Conversion to Bitcoin

- The majority of portions of the stolen Ethereum has now been converted directly into Bitcoin.
- Despite the swift movement of assets, most of the converted Bitcoin remains largely stationary, suggesting that the hackers are preparing for large-scale liquidation or further obfuscation through over-the-counter (OTC) networks.

Graph visualizing the laundering process (as of 2025/2/26)



TRM’s North Korea expert
(A former FBI SME)

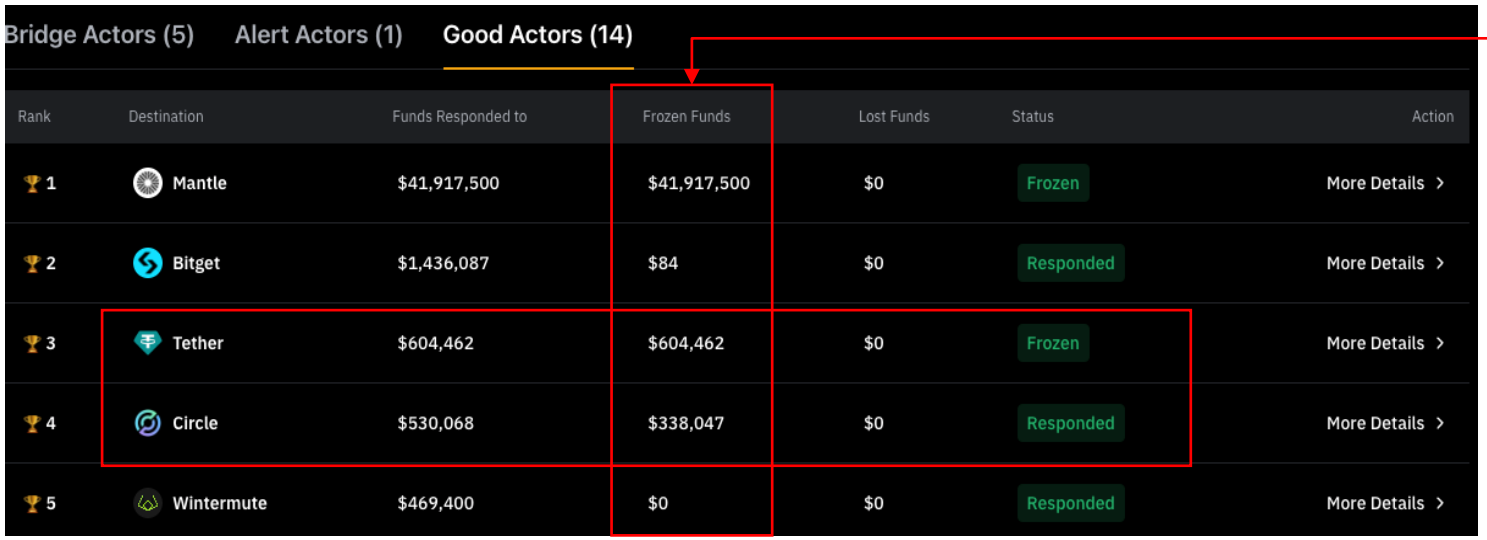
The Bybit exploit indicates that the regime is intensifying its “flood the zone” technique — overwhelming compliance teams, blockchain analysts, and law enforcement agencies with rapid, high-frequency transactions across multiple platforms, thereby complicating tracking efforts.

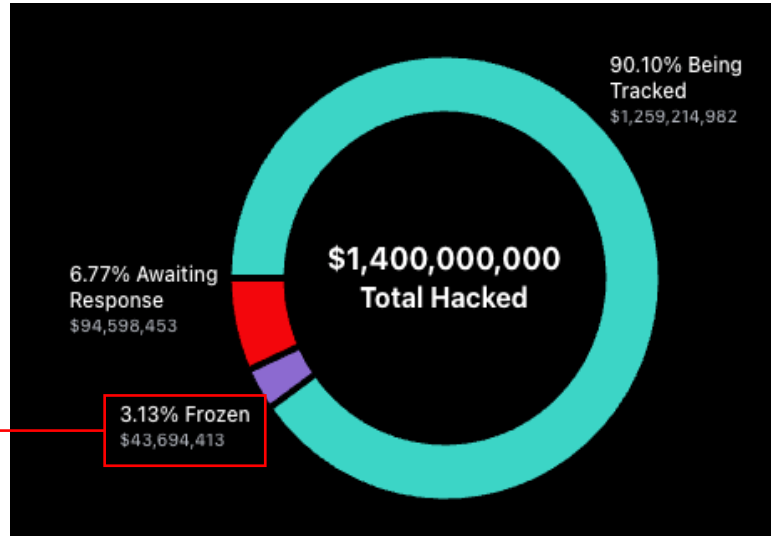
【Source】：「The Bybit Hack: Following North Korea’s Largest Exploit」（TRM Labs）_March 2025

The Bybit Hack - (4) Open investigation to recover hacked funds (Still ongoing as of 2025/3/7)

With the activation of Bybit's bounty recovery program, the industry is working to recover the stolen funds through a cooperative public investigation effort.

- Bybit launched the LazarusBounty program in response to the unprecedented security breach, that aims to incentivize the crypto community to track, trace and freeze the stolen funds, also to encourage exchanges, mixers and other industry players to act swiftly against sanctioned transactions, publicly ranking “good actors” who cooperate and “bad actors” who facilitate illicit activities, thereby setting a new standard for blockchain security.
- As Bybit's CEO shared on his X, Executive Summary on Hacked Funds as of 2025/3/4 states that, total hacked funds of USD 1.4bn around 500k ETH, 77% are still traceable, 20% has gone dark, 3% have been frozen. 83% have been converted into BTC with 6,954 wallets (Average 1.71 btc each) , thus this and the coming week is critical for fund freezing as the funds will start to clear at exchanges, otc and p2p. As for bounty update, $2,178,797 USDT has been paid out to 11 bounty hunters.
- The LazarusBounty website is updating the status of the recovery of the funds in real time. By 2025/3/5 11:00 JST, 3.13% of the hacked funds were frozen, and Tether and Circle, the stablecoin issuers, also contributed to the freezing of the funds.





【Source】：「About Lazarusbounty」(Bybit) , Bybit CEO’s X, 「Lazarusbounty」(Bybit)_March 2025

Deloitte.
デロイト トーマツ

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Risk Advisory LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Group LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With approximately 20,000 people in about 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's more than 450,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, or their related entities(collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited