Crypto-Asset Misuse in Financial Crime: Strategic Findings and Typologies

Cellule de
Renseignement
Financier

PUBLIC VERSION

Contents

Acronyms and abbreviations

CASP	Crypto-Asset Service Provider (as defined by MiCA)
CEX	Centralised Exchange
CIFO	Crypto-In Fiat-Out
CRF	Cellule de Renseignement Financier (FIU Luxembourg)
CSAM	Child Sexual Abuse Material
DeFi	Decentralised Finance
DEX	Decentralised Exchange
DNFBP	Designated Non-Financial Business and Profession
DNM	Darknet Market
FICO	Fiat-In Crypto-Out
FIFO	Fiat-In Fiat-Out
IVTS	Informal Value Transfer System
KYC	Know-Your-Customer
L2	Layer-2
ML	Money Laundering

Acronyms and abbreviations

MMN	Money Mule Network
OTC	Over-the-Counter
PII	Personally Identifiable Information
SAR	Suspicious Activity Report
SARe	Online Providers – Suspicious Activity Report
STR	Suspicious Transaction Report
STRe	Online Providers – Suspicious Transaction Report
TF	Terrorist Financing
TFAR	Terrorist Financing Activity Report
TFTR	Terrorist Financing Transaction Report
URL	Uniform Resource Locator
VASP	Virtual Asset Service Provider (as defined by the FATF)
vIBAN	Virtual International Bank Account Number
web3	Web 3.0

Introduction

Cellule de
Renseignement
Financier

Introduction

The growing use of crypto-assets has been accompanied by an increase in their exploitation for illicit purposes, with criminals leveraging diverse methods, products, and channels to facilitate a wide range of financial crimes.

Over the past few years, Luxembourg's Financial Intelligence Unit (hereafter the "CRF") has been receiving a significant number of Suspicious Activity and Transaction Reports (SARs/STRs) from reporting entities involving the use of crypto-assets for money laundering (ML) or terrorist financing (TF) purposes. These SARs and STRs do not only stem from Crypto-Asset Service Providers (CASPs) or Virtual Asset Service Providers (VASPs), as the misuse of such assets might also be reported by other types of professionals in the context of their different business relationships. Hence, the CRF conducted an analysis of reports received to identify the main typologies, emerging trends and related red flag indicators regarding crypto-assets and financial crime.

The purpose of this strategic analysis is to contribute to a better understanding of the current landscape of ML/TF suspicions relating to the misuse of crypto-assets, with a view to supporting reporting entities and competent public authorities in assessing the ML/TF risks associated with the misuse of crypto-assets from an FIU perspective. Collaboration between public and private stakeholders is particularly important when it comes to fighting financial crime fueled by crypto-assets, especially with regard to the complexity and technicity that underpins some of these schemes.

This strategic analysis is based on a selection of SARs/STRs submitted to the CRF during 2025. The cases examined are intended to provide an overview of the principal ML/TF typologies involving the misuse of crypto-assets, illustrating the products, transaction schemes, persons involved, and selected technical characteristics of the crypto-assets encountered. The analysis is illustrative in nature and should not be understood as an exhaustive or statistically representative account of all SARs/STRs received by the CRF.

Methodology

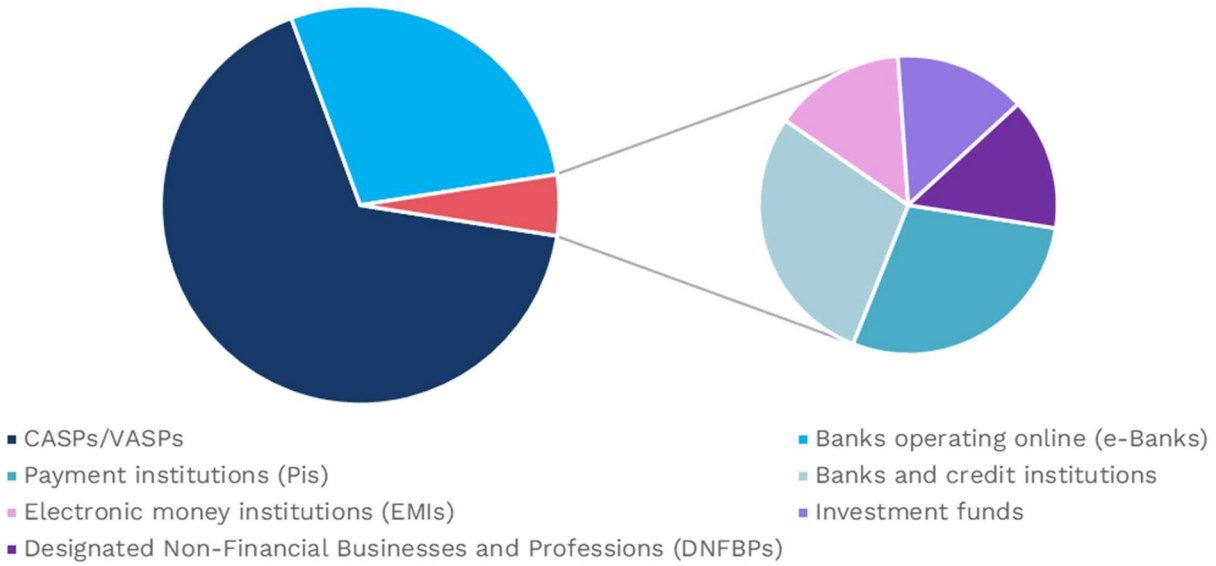
Cellule de
Renseignement
Financier

Methodology

A sample-based methodology was used to conduct this analysis of 2025 reporting on the misuse of crypto-assets for financial crime purposes. Thus, only reports filed with the CRF during the year 2025 are part of the sample. In this context, the notion of "SARs/STRs" refers to different types of filings received from reporting entities, including SARs, STRs, SARe (SARs from online service providers*), STRe (STRs from online service providers) and TFARs (Terrorist Financing Suspicious Activity Reports).

For the sake of representativeness, reports included in the selected sample were submitted to the CRF by different types of reporting entities, including CASPs/VASPs, banks and credit institutions (including online banks), payment institutions, the investment sector and some designated non-financial businesses and professions (DNFBPs).

Distribution of reporting entities in the study sample



*The notion of « online service providers » refers to reporting entity types such as Payment institutions (PIs), Electronic Money Institutions (EMIs), Banks operating online, Virtual Asset Service Providers (VASPs). Although most of these types of professionals submit SARe/STRe, some of them might, for different reasons, submit SARs/STRs instead.

Methodology

The sampling methodology used for this study, including techniques such as keyword search, attribute filtering, stratified sampling, and risk-weighted sampling enabled the identification of the most reported typologies and methods from hundreds of received SARs/STRs, as well as the detection of nascent and emerging trends, directly or indirectly involving crypto-assets. In this context, CEX accounts refer to accounts held by users on a centralised exchange (CASPs/VASPs), allowing them to store, trade, deposit, and withdraw crypto-assets through a platform managed by a central operator.

The multi-dimensional nature of this analysis lies in the fact that the different data points used cover a large set of information available to the CRF, including transactional and financial data, crypto-asset characteristics, customer and geographical attributes, behavioral and temporal features, reporting and trigger elements.

Less than 10% of the study sample referred to Luxembourg residents as subject persons of SARs/STRs, which is in line with Luxembourg's role as an international financial center, highlighting the cross-border nature of most transactions, including those directly or indirectly involving crypto-assets and related services.

All statistics presented in this document are based on a study sample of SARs/STRs related to crypto-assets submitted to the CRF during 2025. As the analysis does not encompass all SARs/STRs received by the CRF, the figures presented are intended solely to illustrate observations derived from the selected sample and should not be interpreted as reflecting the overall volume or level of reporting to the CRF in relation to crypto-assets.

Key findings

Cellule de
Renseignement
Financier

Key findings

Five key highlights on the misuse of crypto-assets in financial crime in 2025 can be drawn from the analysis :

1

BTC AND ETH STILL DOMINATE

When it comes to ML/TF suspicions using crypto-assets, cryptocurrencies (BTC, ETH) dominate. More than 60% of cases involved the use of cryptocurrencies, out of which 90% involved BTC, ETH or both.

2

STABLECOINS ARE INCREASINGLY BEING USED

The analysis identified stablecoins as the second most used type of crypto-asset due to their relative price stability and widespread usage in many market transactions, including cross-border transfers, remittances and for on/off ramp purposes. Their usage often remains coupled with native cryptocurrencies.

3

PROMINENT ROLE OF FRAUD SCHEMES

Among the SARs/STRs providing sufficient information on the origin of funds, many suspected illicit crypto-asset-related funds were linked to scams and other forms of fraud.

4

A VARIETY OF PRODUCTS AND CHANNELS

Given that most analysed SARs/STRs were filed by VASPs/CASPs, the frequent identification of personal CEX accounts reflects the composition of the sample. Other products observed include vIBANs, corporate CEX accounts, online bank accounts, and e-money/payment accounts used in combination with crypto-assets for ML/TF purposes.

5

SUSPICIOUS ACTIVITY IS LARGELY CROSS-BORDER

The majority of ML/TF suspicions in 2025 related to the use of crypto-assets involved non-resident EU individuals as subject persons, with funds transiting Luxembourg as the host country for the accounts and products used.

Crypto-asset ecosystem and definitions

Cellule de
Renseignement
Financier

Crypto-assets

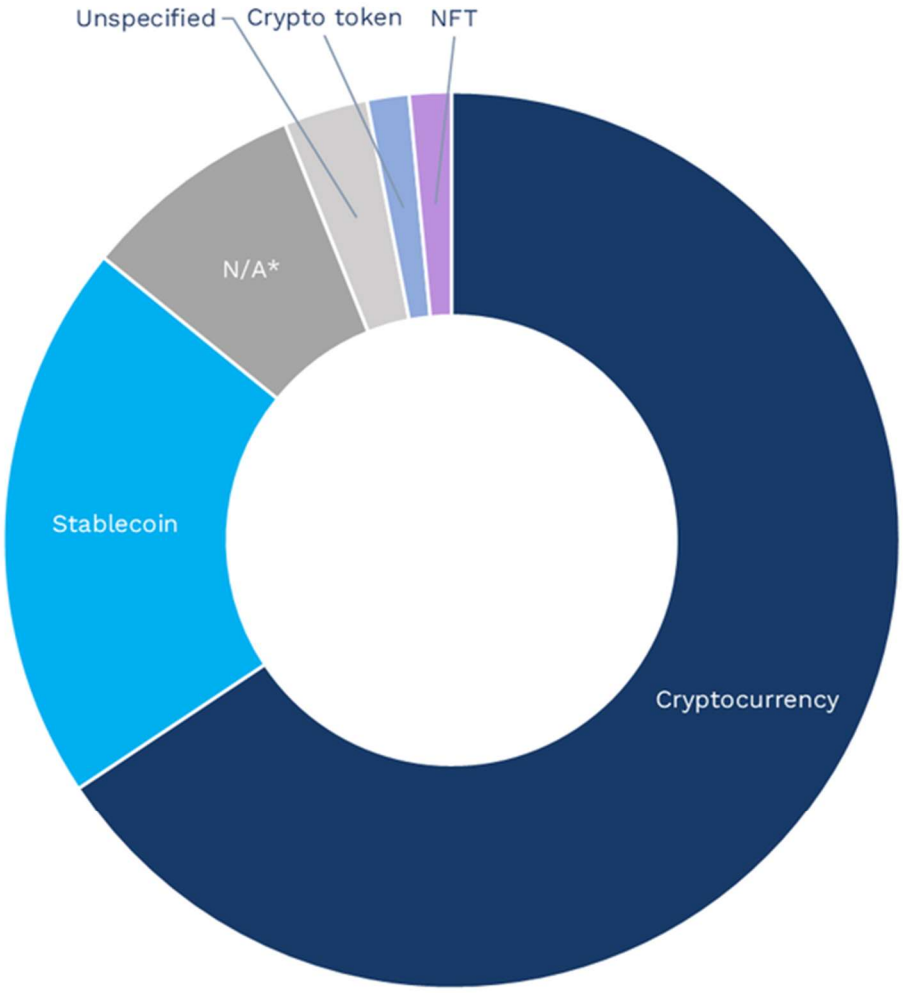
In the context of this strategic analysis on the misuse of crypto-assets for ML/TF purposes, it is useful to distinguish between four main types of crypto-assets:

Crypto-asset type	Characteristics	Examples
Cryptocurrency	Native coin, i.e. built-in currency running on its own blockchain	Most frequently identified cryptocurrencies include BTC, ETH, XRP, SOL
Crypto token	Non-native coin, i.e. running on an existing blockchain using smart contracts	Most frequently identified crypto tokens include DTCoin, LINK, WBTC
Non-fungible token (NFT)	Unique virtual asset recorded on a blockchain and used to represent ownership of a specific term or piece of content	NFTs are various by nature and specific to different types of projects and contents
Stablecoin	Cryptocurrencies or tokens pegged to a reference asset such as a fiat currency	Most frequently identified stablecoins include USDC (USD Coin) and USDT (Tether)

Crypto-assets

The breakdown of crypto-assets identified in the reviewed cases shows that, within the 2025 study sample, cryptocurrencies (native coins) were the most frequently observed crypto-asset type in relation to ML/TF purposes, followed by stablecoins.

Breakdown of crypto-asset types in SARs/STRs relating to the misuse of crypto-assets in 2025 (study sample)



* “N/A” (not applicable) refers to cases where crypto-asset-related services and accounts were used with the purpose of using crypto-assets, but without any specific crypto-asset being actually involved at time of reporting.

ML/TF typologies

Cellule de
Renseignement
Financier

Typology categories

The review of 2025 reporting of SARs/STRs relating to the misuse of crypto-assets enabled the identification of five main ML/TF typology categories:

- **Money Laundering through Crypto-Assets** (the use of crypto-assets to reroute funds from their original source for ML/TF purposes),
- **Crypto-Asset-Based Fraud and Abuse** (the use of crypto-assets and related services to funnel or conceal proceeds of fraudulent activities, including schemes beyond self-laundering),
- **Illicit Fund Movement via Intermediaries** (the use of third parties, such as unregulated service providers, personal accounts and crypto money mules, or temporary wallets, to obscure the origin, destination, or ownership of illicit funds),
- **Indirect Exposure to Illicit Addresses** (subjects being indirectly exposed to illicit actors such as sanctioned entities, darknet markets without direct interaction, through intermediary wallets or entities),
- **Direct Interactions with Illicit Addresses** (direct unmediated transactions with crypto addresses linked to illicit activities, such as darknet markets, fraud or terrorist financing).

Each typology category is divided into subcategories covering more specific ML/TF schemes involving the direct or indirect use of crypto-assets. These categories and subcategories were identified through a cross-analysis of transactional, financial, behavioural, temporal and product-related data.

Typology subcategories

Details relating to each typology subcategory, their respective characteristics and the methods used are described in this strategic analysis report.

ML/TF typology categories and subcategories from SARs/STRs relating to the misuse of crypto-assets in 2025 (study sample)

Money Laundering through Crypto-Assets	Crypto-Asset-Based Fraud and Abuse	Illicit Fund Movement via Intermediaries	Indirect Exposure to Illicit Addresses	Direct Interactions with Illicit Addresses
Money Laundering via Crypto Investments	Victim-Facilitated Laundering via Wallet Hopping	Transit Account Activity Involving Crypto Platforms	Darknet Markets	
Crypto Laundering via Real Estate Investments	Account Takeover	Money Mule Activity Involving Crypto Platforms	Indirect Exposure to Sanctioned Entities	Sale of Drugs
Professional-to-Personal Asset Diversion via Crypto Investments	Fake or Suspicious Crypto Platform	Money Mule Activity Involving NFTs	Indirect Exposure to CSAM Addresses	Purchase of CSAM Content
	Investment Scam		Indirect Exposure to Ransomware and Stolen Funds Clusters	Scam Addresses and Platforms
	Fraudulent Account & Identity Theft		Indirect Exposure to TF Addresses	

Money laundering through crypto-assets

In the context of this strategic analysis, “money laundering through crypto-assets” refers broadly to the use of crypto-assets to move, convert or conceal funds whose origin or intended use raises suspicion. The identified schemes typically involve crypto-asset trading accounts or wallets held with centralised exchanges (CEXs), which may be used alongside bank accounts and products such as virtual IBANs (vIBANs) to facilitate transfers between the fiat and crypto-asset ecosystems.

Although the available information does not always allow the underlying predicate offence to be identified, the nature of the transactions, the movement of funds between fiat and crypto-assets, and the surrounding circumstances generally give rise to suspicions of money laundering.

This category is divided into three subcategories:

1	Money Laundering via Crypto Investments
2	Crypto Laundering via Real Estate Investments
3	Professional-to-Personal Asset Diversion via Crypto Investments

Money laundering through crypto-assets

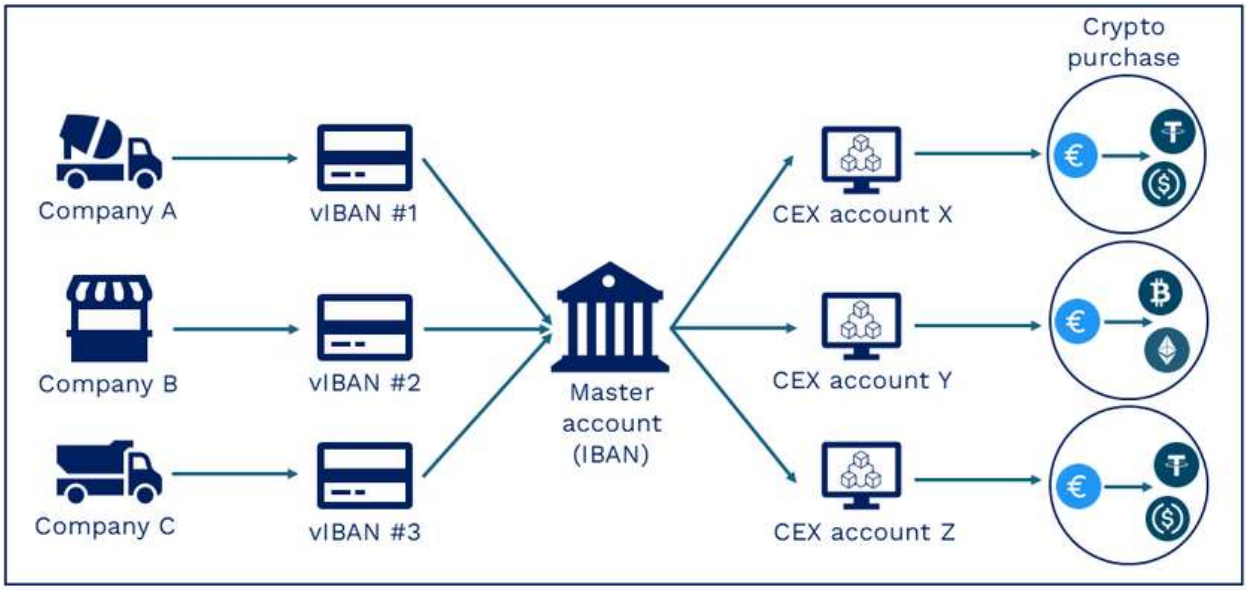
1. Money Laundering via Crypto Investments

This typology subcategory covers the actual or intended conversion of fiat currency into crypto-assets, primarily cryptocurrencies and stablecoins. In the cases concerned, the source of the fiat funds was unclear, while the stated purpose of the conversion appeared inconsistent with the subject's business activity.

The cases mainly involved foreign commercial companies based in Europe and operating in sectors such as construction, transportation and wholesale. In some instances, these companies used vIBANs to transfer significant amounts of fiat currency—often within a short period—to their own trading accounts held with legitimate CEXs. The vIBANs served only as a payment channel: once the funds reached the CEX accounts, they were converted into cryptocurrencies or stablecoins, mainly USDT or USDC.

The companies generally stated that these conversions were intended to settle business invoices or support treasury-management activities.

Illustration: Suspicious vIBAN-to-CEX on-ramp flows



Money laundering through crypto-assets

2. Crypto Laundering via Real Estate Investments

Real estate investment may be used to launder illicit proceeds held in crypto-assets. As an example, criminals may convert crypto-assets into fiat and use the funds as an equity contribution towards a loan-financed property purchase.

Such schemes may be identified through due diligence conducted by the obliged entities and professionals involved, including CASPs/VASPs, banks, credit institutions and notaries.

3. Professional-to-Personal Asset Diversion via Crypto Investments

Personal CEX accounts or wallets also feature in ML schemes linked to tax crime or the misuse or misappropriation of company assets. In such cases, legitimate business revenues may be transferred from a company bank account to an individual's personal CEX account or wallet and subsequently converted into crypto-assets.

Depending on the circumstances, these transactions may be intended to divert company funds for personal benefit and/or to conceal taxable business income from the relevant tax authorities.

Such schemes may also involve the provision of false tax-residency information for purposes of tax crime.

Crypto-asset-based fraud and abuse

The “Crypto-Asset-Based Fraud and Abuse” category covers a range of ML schemes in which crypto-assets are used to transfer or conceal proceeds derived from fraud, including scams. Unlike fraud-derived self-laundering, discussed in the “Money Laundering through Crypto-Assets” section, this category is not limited to schemes carried out by the perpetrators of the underlying fraud themselves (self-laundering ML schemes).

This category is subdivided into five different subcategories:

1	Victim-Facilitated Laundering via Wallet Hopping
2	Account Takeover
3	Fake or Suspicious Crypto Platform
4	Investment Scam
5	Fraudulent Account & Identity Theft

Crypto-asset-based fraud and abuse

1. Victim-Facilitated Laundering via Wallet Hopping

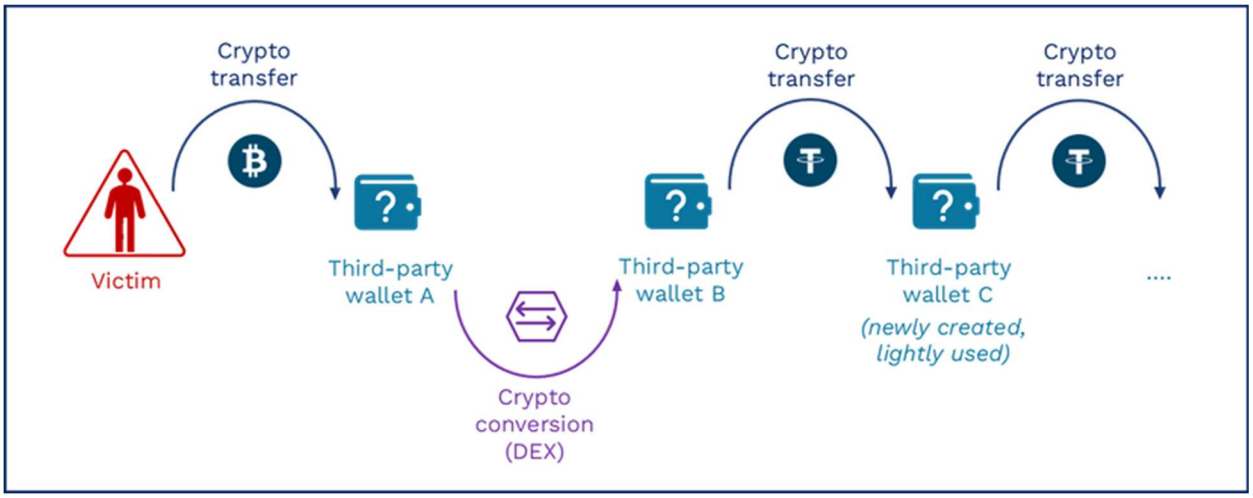
Wallet hopping refers to the rapid or successive transfer(s) of crypto-assets through multiple wallets. These wallets may often be newly created, lightly used, or seemingly unrelated to each other.

While wallet hopping does not necessarily mean that ML or TF is occurring, there may be reasons to suspect potential ML/TF activities when wallet hopping is used along tumblers and/or mixers, high-risk services, cross-chain bridges, or successive attempts to off-ramp.

The analysis conducted on the 2025 sample data, shows that SARs/STRs submitted to the CRF involving crypto wallet hopping were often linked to funds being transferred through multiple wallets, initially stemming from defrauded individuals' CEX accounts.

Typically, such patterns consist of victims sending amounts ranging from EUR 100 to several hundred thousand euros of cryptocurrencies (ETH, BTC) in several transactions to addresses from which funds are subsequently further funneled, split and converted to stablecoins or other cryptocurrencies using services such as decentralised exchange (DEX) platforms, instant crypto exchanges (*swapping*) and non-custodial wallets. Once converted, the funds may end up being linked to known scam-related wallet clusters, which can significantly facilitate the identification of potential fraudulent schemes.

Illustration: Victim-facilitated wallet hopping through third-party wallets



Crypto-asset-based fraud and abuse

2. Account Takeover

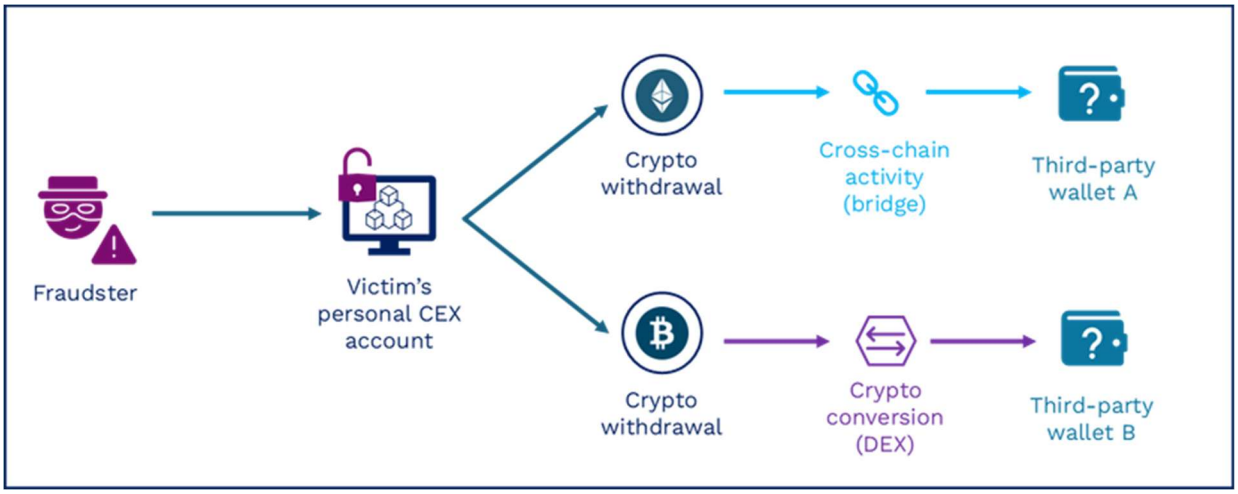
Account takeover (ATO) occurs when criminals gain unauthorised access to a user's online account. It may affect banking, email and e-commerce services, as well as crypto-asset platforms and wallets. Most crypto-asset-related ATO cases identified in the 2025 study sample involved personal CEX accounts holding cryptocurrencies such as BTC and ETH. These accounts were compromised through methods including phishing links or websites and voice phishing (vishing). Once access had been obtained, the fraudsters typically transferred the crypto-assets within a very short period to third-party wallet addresses. In most cases, these addresses had first been whitelisted by the fraudsters to reduce the likelihood of the transactions being blocked or subject to additional verification.

The stolen funds may be transferred to addresses associated with other centralised exchanges (CEXs) as well as to swap services and decentralised protocols. The funds may then be split across multiple addresses and converted into other crypto-assets to further obscure their illicit origin.

Some crypto-asset ATO schemes also involved cross-chain activity, with bridges used to transfer stolen funds from one blockchain network to another, for example from Ethereum to TRON.

Further information on cross-chain activity is provided in the "Emerging Trends" section of this report.

Illustration: CEX account takeover with cross-chain and DEX-based transfers



Crypto-asset-based fraud and abuse

3. Fake or Suspicious Crypto Platform

In addition to fraudulent transaction schemes, account takeovers (ATO) and investment scams, the study sample identified cases involving fake or highly suspicious crypto-asset exchange platforms and websites. These platforms may be used either independently to deceive victims or in combination with other fraud typologies.

When combined with previously mentioned typologies, fake crypto exchange platforms may act as a catalyst for further fraud.

For instance, victims of investment scams were tricked by fake crypto exchange platforms into sending cryptocurrencies in exchange of a promised financial reward. Moreover, investment scams powered by fake crypto exchange platforms also facilitate the perpetration of other types of fraud, for example *recovery fraud*. In such cases, scammers promise their victims a chance to retrieve their funds in exchange of an additional cryptocurrency withdrawal to allegedly cover the fee of the corresponding smart contract. As the victims follow the transaction link and fund the wallet, they once again get scammed as fraudsters take hold of their wallet and funds.

In other situations, some victims got redirected toward fraudulent crypto investment websites in the context of online romance scams, with scammers initially luring their victims from mobile dating apps and fraudulent websites (URLs) subsequently shared via instant messaging apps.

4. Investment Scam

Another type of fraud identified in SARs/STRs submitted in 2025 relating to crypto-assets is *investment scam*, which revolves around schemes promising high, guaranteed returns with little to no risk for the investor.

When it comes to the involvement of crypto-assets, this phenomenon primarily targets CEX individual account users. From a transactional perspective, this is reflected by victims sending significant amounts of cryptocurrencies (e.g., ETH) and/or stablecoins (e.g., USDC, USDT) to scam-related addresses within a relatively short time frame.

Crypto-asset-based fraud and abuse

4. Investment Scam (cont'd)

Similarly to other types of ML/TF typologies pertaining to the misuse of crypto-assets, the transferred funds are subsequently funneled through various intermediary addresses from other CEXs.

Furthermore, victims sometimes received in return small amounts (in euros) from the scam address, which is part of the scam strategy, with small returns being promised to the victims to encourage further crypto investments. In addition to transactional elements that enable an easier identification of crypto-asset-related investment scams, claims from the victims themselves also helped identify similar patterns.

5. Fraudulent Account & Identity Theft

Some crypto-asset-related SARs/STRs concern fraudulent CEX accounts opened using fictious or stolen identities. These accounts may be detected during onboarding when applicants submit forged or stolen identity documents. However, AI-generated identity documents and deepfakes used to circumvent identity-verification checks are more difficult to detect.

Once opened, fraudulent accounts may use payment services integrated into crypto-asset exchange platforms to convert fiat currency into crypto-assets. The acquired crypto-assets may then be transferred to services accessible through encrypted instant-messaging applications, some of which apply limited or no Know-Your-Customer (KYC) measures and allow users to trade or store crypto-assets with greater anonymity.

In addition to the detection of forged or stolen identity documents, customer data and technical metadata can help identify clusters of fraudulent CEX accounts. For example, multiple suspicious accounts sharing the same residential address, recurring IP addresses or device identifiers may indicate that they are being controlled by the same individual or organised group for illicit purposes.

Illicit fund movement via intermediaries

This category covers schemes designed to conceal the origin, destination or ownership of illicit funds – typically held as crypto-assets – by routing them through a series of intermediaries. These may include third-party accounts, individuals, unregulated service providers or informal exchange arrangements.

Rather than transferring funds directly from their source to their ultimate destination, criminals use third parties, either knowingly or unknowingly, to create additional layers between themselves and the proceeds of crime. Within the crypto-asset ecosystem, such methods may involve interposed personal accounts, temporary wallets or unregulated exchange mechanisms intended to obscure transaction flows. Almost half of the cases involving intermediated movements of illicit crypto-assets included the use of money mules.

This category is subdivided into four different subcategories:

1	Transit Account Activity Involving Crypto Platforms
2	Money Mule Activity Involving Crypto Platforms
3	Money Mule Activity Involving NFTs

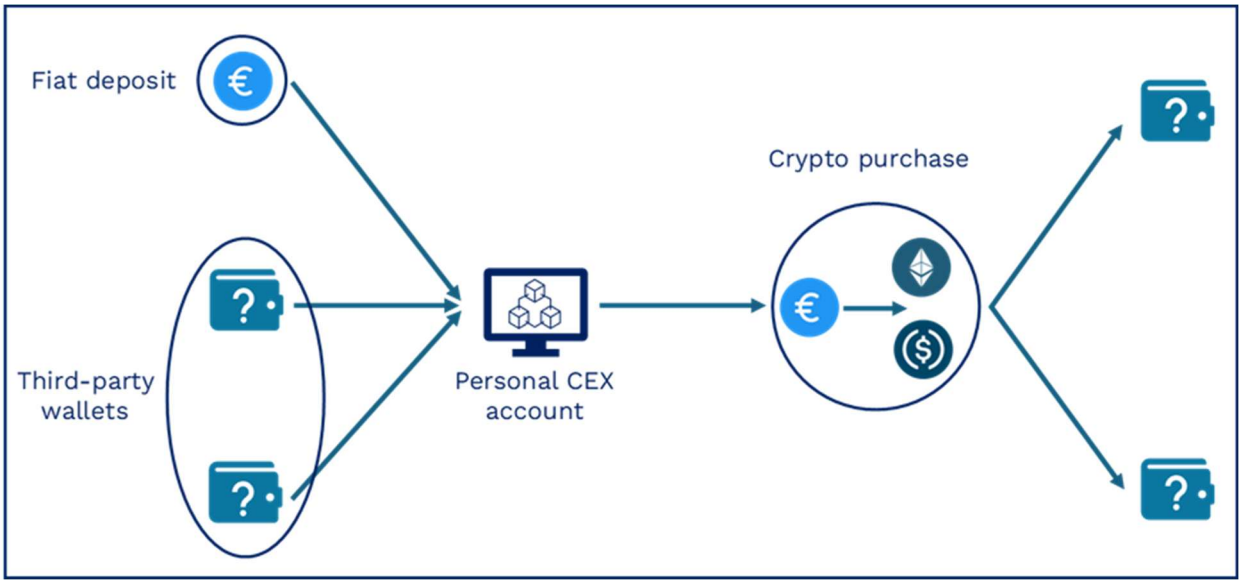
Illicit fund movement via intermediaries

1. Transit Account Activity Involving Crypto Platforms

In an ML/TF context, a transit or pass-through account is generally understood as an account used primarily to receive and rapidly transfer funds. For crypto-assets, the SARs/STRs reviewed indicate that illicit transit activity mainly involves personal crypto-asset trading accounts held with CEXs. These accounts are used to convert fiat currency into crypto-assets or to move crypto-assets between wallets and platforms.

The accounts are typically funded either through on-ramping, whereby fiat currency is deposited and used to purchase cryptocurrencies or stablecoins, or through incoming crypto-asset transfers from seemingly unrelated third-party wallets. The funds are then transferred onwards within a short period of time. Their suspected sources include proceeds from predicate offences such as scams and drug trafficking.

Illustration: Suspicious on-ramp activity through a CEX transit account



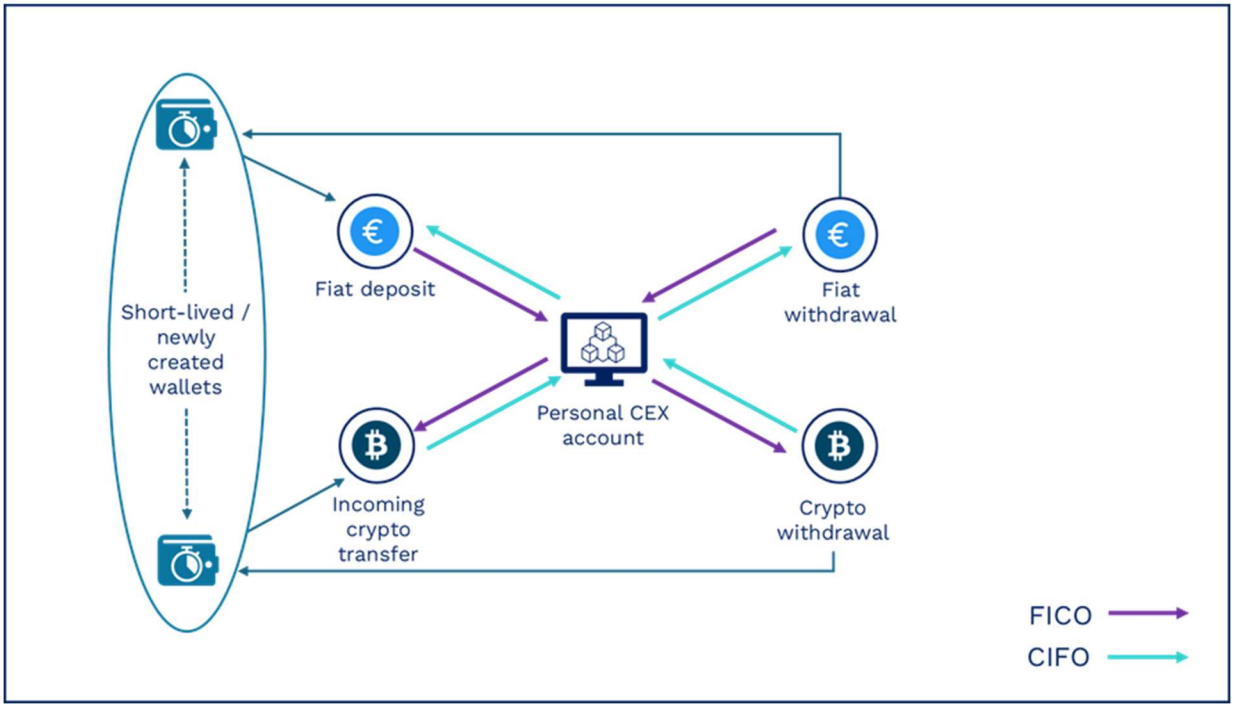
A key characteristic of such transit CEX accounts is the recurrence of FICO (fiat-in crypto-out), CIFO (crypto-in fiat-out) and circular transactional patterns, reinforcing money laundering suspicions.

Illicit fund movement via intermediaries

1. Transit Account Activity Involving Crypto Platforms (cont'd)

FICO and CIFO patterns using CEX accounts may raise suspicions on the source of funds involved, irrespective of their form (fiat or crypto), especially when coupled with elements indicating that these might be used as transit or pass-through accounts, such as short-lived or newly created wallets, consecutive use of FICO and/or CIFO patterns, or significant amounts transacted sporadically within a short period of time.

Illustration: Recurrent FICO and CIFO patterns through a transit CEX account



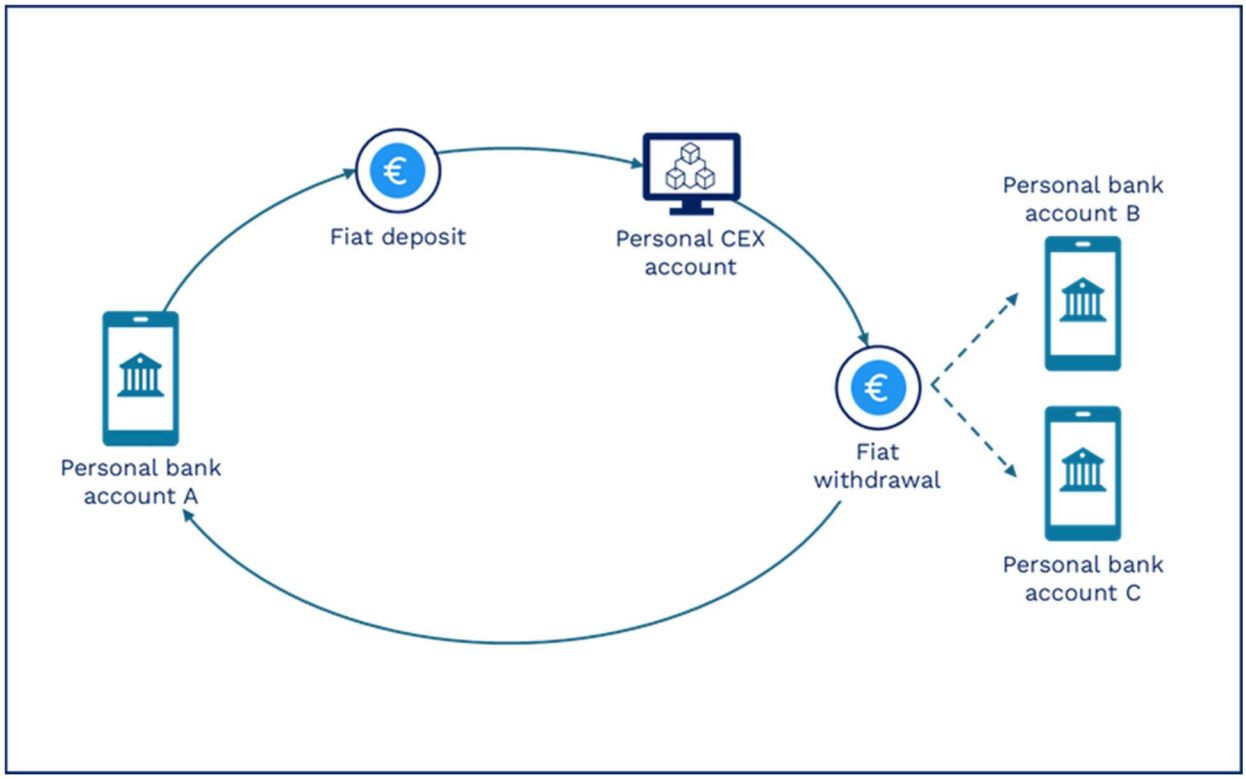
As noted above, CEX accounts used as transit or pass-through accounts may receive funds suspected of deriving from drug trafficking or other criminal activities. Cases involving individuals with suspected links to drug traffickers or associated criminal networks displayed a similar transaction pattern: large incoming crypto-asset transfers or fiat deposits from unclear sources were followed almost immediately by withdrawals to unlabelled external wallets. Although the origin of the funds often remained unclear, some cases involved foreign shell companies or retail businesses suspected of acting as fronts.

Illicit fund movement via intermediaries

1. Transit Account Activity Involving Crypto Platforms (cont'd)

When it comes to fraud or scam, circular transactions occur when perpetrators deposit small amounts of fiat currency from a bank account into a CEX account and, without converting the funds into crypto-assets, transferring them back to the originating bank account or to another account under their control. Such a pattern is referred to as FIFO (fiat-in fiat-out). After that, no additional login or further CEX account activity is observed. This behavior reflects the use of the CEX account simply as a conduit rather than for legitimate trading or investment.

Illustration: Fraud-related FIFO activity using a CEX transit account



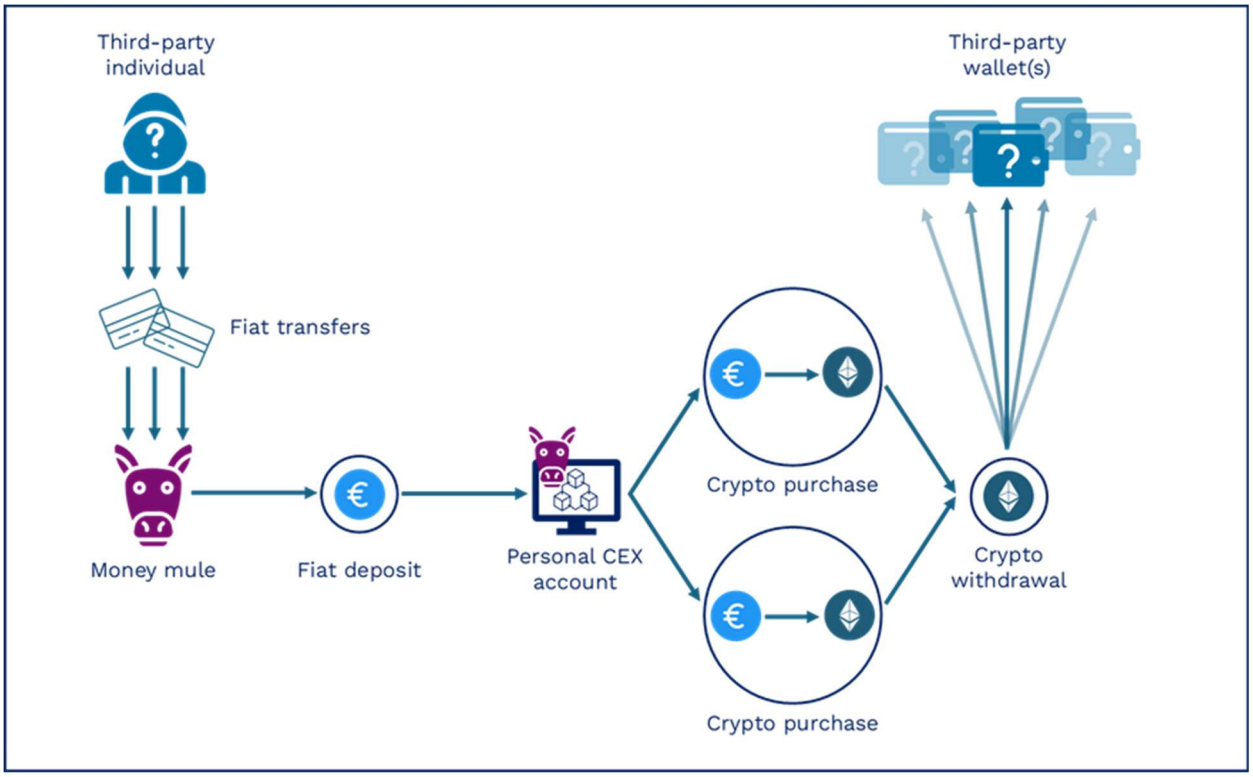
Illicit fund movement via intermediaries

2. Money Mule Activity Involving Crypto Platforms

A *money mule* is a person who transfers or moves ill-gotten funds on behalf of other individuals. While many are knowingly recruited, often through online channels, some of them may participate unwittingly.

Within the crypto-asset ecosystem, money mules are individuals who use their accounts and payment instruments to receive and transfer illicit funds on behalf of third parties. The cases reviewed included EU nationals using a combination of personal CEX accounts, crypto-asset wallets, credit cards, online payment accounts and bank accounts. Funds received from unknown or seemingly unrelated third parties may be transferred onwards through payment service providers, other CEXs — including non-custodial instant exchanges — or virtual debit cards. Where such transactions are declined, the mules may reroute the funds through accounts or wallets held by additional, unrelated third parties.

Illustration: Crypto money mule activity and third-party wallets



Illicit fund movement via intermediaries

3. Money Mule Activity Involving NFTs

In more specific cases, NFT purchases have been suspected of facilitating money laundering activities. For example, non-resident individuals (suspected money mules) opened and used e-money accounts to acquire NFTs via exchange platforms, with transactional activities being indicative of pass-through accounts and layering typologies, as incoming funds were coming from unrelated third parties in various countries, followed by immediate transfers to other accounts and subsequent NFT purchases.

Indirect exposure to illicit addresses

This section focuses on cases reported to the CRF relating to indirect exposure with illicit crypto addresses, wallets, or address clusters. From a crypto-asset perspective, indirect exposure means exposure to funds, wallets, or entities that are themselves linked to a risky source, even though the subjects did not transact with the source directly. For instance, illicit addresses are those linked to sanctioned entities, child sexual abuse material (CSAM), terrorist financing (TF), darknet markets or other illicit activities. Indirect exposure may be incoming, where funds move from an illicit address towards the subject through one or more intermediary addresses, or outgoing, where funds move from the subject towards an illicit address through such intermediaries. Such exposure is usually uncovered using blockchain analytics tools. While this exposure may constitute a risk indicator, it does not, on its own, establish that the transactions were conducted for ML/TF purposes.

This category is subdivided into five different subcategories.

1	Indirect Exposure to Sanctioned Entities
2	Indirect Exposure to CSAM Addresses
3	Indirect Exposure to Ransomware and Stolen Funds Clusters
4	Darknet Markets
5	Indirect Exposure to TF Addresses

Indirect exposure to illicit addresses

1. Indirect Exposure to Sanctioned Entities

Cases reported in 2025 involved EU-residents and companies, including crypto-asset exchanges, whose CEX accounts showed indirect incoming or outgoing exposure to sanctioned entities. The relevant foreign crypto-asset exchanges were either themselves subject to international restrictive measures or associated with jurisdictions subject to such measures. In most reviewed cases, these were sanctions lists issued by foreign countries.

The amounts linked to this exposure were generally low, and the transactions passed through several intermediary addresses before reaching the subject or the sanctioned entity, resulting in multi-hop exposure. Although indirect exposure to a sanctioned crypto-asset exchange constitutes a risk indicator, it does not, on its own, demonstrate money laundering or sanctions evasion, as the connection may be incidental or unintentional.

2. Indirect Exposure to CSAM Addresses

Child sexual abuse material (CSAM), formerly commonly referred to as “child pornography”, comprises visual material depicting the sexual abuse or exploitation of children. Due to its illegal nature, persons seeking to access or distribute CSAM often rely on tools and channels offering greater anonymity. Crypto-assets may therefore be used to pay for such material or otherwise facilitate its distribution.

Among the cases of indirect exposure reported in 2025, certain CEX accounts showed indirect outgoing exposure to CSAM-linked addresses. Crypto-assets were withdrawn to intermediary addresses—primarily unlabeled wallets—before being transferred onwards to addresses associated with CSAM. The transaction paths were generally short, with some CSAM-linked destination addresses located only one hop away from the originating CEX account.

Indirect exposure to illicit addresses

3. Indirect Exposure to Ransomware and Stolen Funds Clusters

This typology describes patterns where CEX account holders deposit cryptocurrencies with indirect incoming exposure to stolen-funds clusters (including ransomware) and mixing services, followed by rapid conversion to fiat and withdrawal to a bank account. Observed *peel chains* are relatively long in order to further obfuscate source of funds and complicate tracing.

As previously noted, indirect exposure alone does not necessarily confirm laundering. Nevertheless, the combination of a notable share of the transaction value traced to stolen-funds clusters, mixing services, multi-hop layering and rapid fiat cash-out constitutes a risk pattern consistent with crypto-enabled laundering. Although ransomware and stolen-funds flows are primarily ML-linked, the same obfuscation methods can be used for a broad range of illicit financing typologies.

4. Darknet Markets

Darknet markets (DNMs), also known as dark web marketplaces, enable the peer-to-peer (P2P) sale and provision of illicit products or services, such as narcotics and other illicit drugs, stolen accounts and data, hacking tools, and fraudulent documents. Submitted SARs/STRs showed that some EU-based CEX account users had incoming or outgoing exposure to various DNMs via cryptocurrency transactions which were typically routed through relatively long peel chains. Moreover, in some cases, such exposure is likely to be intentional as several high-risk transaction paths repeatedly converged at the subject's account.

5. Indirect Exposure to TF Addresses

A limited number of SARs/STRs in the study sample showed indirect outgoing exposure to addresses linked to potential TF activity. These addresses formed part of clusters whose root addresses had been attributed to foreign terrorist groups reportedly affiliated with larger international terrorist organizations.

Such outgoing indirect exposure consists of cryptocurrencies stemming from CEX accounts held by foreign crypto exchanges acting on behalf of users and being routed through a very small number of intermediate addresses and involving small amounts.

Direct interactions with illicit addresses

Unlike indirect exposure typologies, this category involves direct and unmediated transactions with illicit crypto addresses, wallets, or address clusters associated with CSAM content, darknet markets (DNMs) and scams. Despite occurring in only a small number of reviewed cases, such direct interactions significantly increase the plausibility of intentional involvement, resulting in stronger suspicions regarding the persons concerned. In this regard, most used types of crypto-assets include cryptocurrencies such as BTC, with individual amounts typically relatively low, below EUR 1,000.

This category is subdivided into four different subcategories:

1	Purchase of CSAM Content
2	Darknet Markets
3	Sale of Drugs
4	Scam Addresses and Platforms

Direct interactions with illicit addresses

1. Purchase of CSAM Content

Outgoing direct exposure to CSAM-related addresses in SARs/STRs in 2025 showed that involved subjects were mostly EU-residents, using their personal CEX account to send BTCs directly to addresses belonging to online platforms distributing CSAM-related content. In these cases, withdrawals are usually made on a one-off basis and amount to an average of less than EUR 100 per transaction.

2. Darknet Markets

EU-residents have been using their CEX accounts to directly and repeatedly receive or withdraw cryptocurrencies (LTC, BTC) from or to DNMs known for being related to online drug shops, bot shops or mixing services, and subsequently cashed out the received funds to foreign EU-based bank accounts.

3. Sale of Drugs

Although limited, a number of reported cases involved EU-based CEX account users directly interacting with drug vendors' wallets in the context of BTC transactions.

4. Scam Addresses and Platforms

Some EU-based CEX account users have been directly transacting with scam-related addresses linked to various fraudulent websites and platforms using cryptocurrencies. While these cases show that crypto-assets may facilitate transactions with scam-related addresses and platforms, available information did not systematically allow confirmation of the users' intent or victim status. Some of the scams involved likely originated on social media platforms: scammers tricked individuals — using deepfake videos of celebrities — into depositing cryptocurrencies on fraudulent websites by promising subsequent giveaways and special promo codes.

Conclusion

Conclusion

Within the limits of the study sample, the analysis suggests that the suspected misuse of crypto-assets for ML/TF purposes remains more prevalent in certain sectors of activity, while the schemes identified show signs of growing technical complexity and the use of an increasingly diverse range of products.

Although cryptocurrencies such as Bitcoin and Ethereum continue to dominate SAR/STR reporting, stablecoins are playing an increasingly significant role. At the same time, the use of products such as virtual IBANs illustrates the growing interconnection between the traditional financial system and the crypto-asset ecosystem, in which criminals and fraudsters exploit both on-chain and off-chain channels to facilitate illicit transactions.

The analysis shows that crypto-assets are used in suspected stand-alone ML schemes, including cases in which the underlying predicate offence could not be identified. Where a predicate offence was identified, fraud-related proceeds were particularly prominent, with social-engineering fraud, investment scams and cyber-enabled fraud representing the main identified sources of illicit funds entering the crypto-asset ecosystem.

While most crypto-asset-related SARs/STRs in the 2025 study sample involved accounts held with centralised exchanges, the suspicious activity observed also pointed to the use of more sophisticated techniques and infrastructure. These included no-KYC swap services, instant exchanges and decentralised platforms, as well as the integration of cross-chain bridges and Layer 2 (L2) networks into suspected laundering schemes. The emerging patterns further illustrate how criminal actors may exploit limited familiarity with the crypto-asset environment and use the technical features of blockchain systems to facilitate illicit activity.

Conclusion

All in all, the crypto-asset ML/TF risk landscape is expanding along multiple vectors: technically, operationally, and structurally, while the profile of subjects involved remains largely international.

Hence, cross-border cooperation, cross-sectoral and cross-product risk considerations, as well as blockchain analytics capabilities will remain essential to detect, trace and disrupt crypto-enabled ML/TF activities.

Disclaimer

The data contained in this document should not be interpreted as operational disclosures, legal opinions, or confidential information relating to ongoing or past investigations. Any use of the content must respect its informative context and may not in any way undermine the mission, security, or integrity of the CRF's work. For any questions regarding this document, please contact the CRF.

Contact

Cellule de Renseignement Financier (CRF)
Email address: crf@justice.etat.lu
Website: www.crf.lu

Ref. SA-CA-PB-2026

August 2026

PUBLIC VERSION

Cellule de Renseignement Financier