Chainalysis

JULY 2024

Money Laundering and Cryptocurrency

Trends and new techniques for detection and investigation

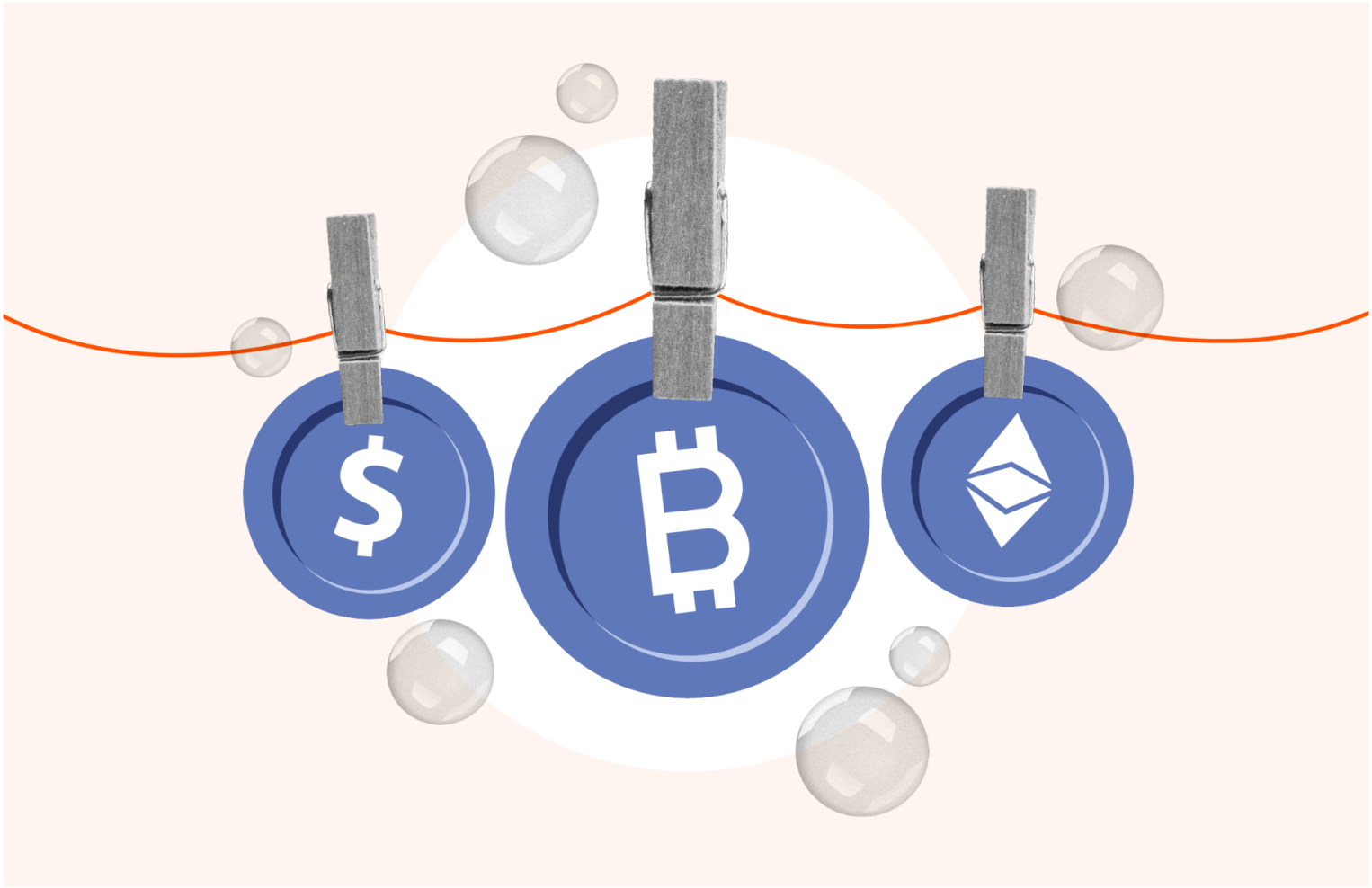


Table of Contents

Money Laundering and Cryptocurrency

While public blockchains are inherently transparent and traceable, illicit actors turn to cryptocurrencies to launder ill-gotten gains for the same reasons people use them for legitimate purposes: they are cross-border, virtually instant, and generally inexpensive to transact. Money laundering in the crypto context is typically associated with cybercriminals attempting to conceal the flow of funds related to on-chain crimes, such as darknet market and ransomware operations. However, cryptocurrency is increasingly being used to launder funds from a broader range of illicit activities beyond the conventional understanding of crypto crime. The growing ubiquity of crypto has made it a tool for laundering proceeds from various off-chain crimes, such as narcotics trafficking and fraud. In 2024, money laundering in crypto encompasses all crime — not just that which is inherently tied to the crypto ecosystem.

This shift carries significant implications for investigators. First, expertise in cryptocurrency must extend beyond specialized cybercrime units to include law enforcement agencies of all kinds. Cryptocurrency is now one of the payment methods used by illicit actors worldwide, and therefore this expertise must encompass both blockchain transaction tracing and a comprehensive understanding of traditional money laundering tactics. Second, there is a silver lining: with the right data and tools, investigators in the public and private sectors can leverage the transparency of blockchain to uncover illicit activity that may otherwise go undetected. Blockchain analysis can generate both intelligence signals for proactive lead generation and more concrete evidence of illicit flows in existing investigations, helping a broad range of analysts and investigators unravel increasingly sophisticated money laundering networks.

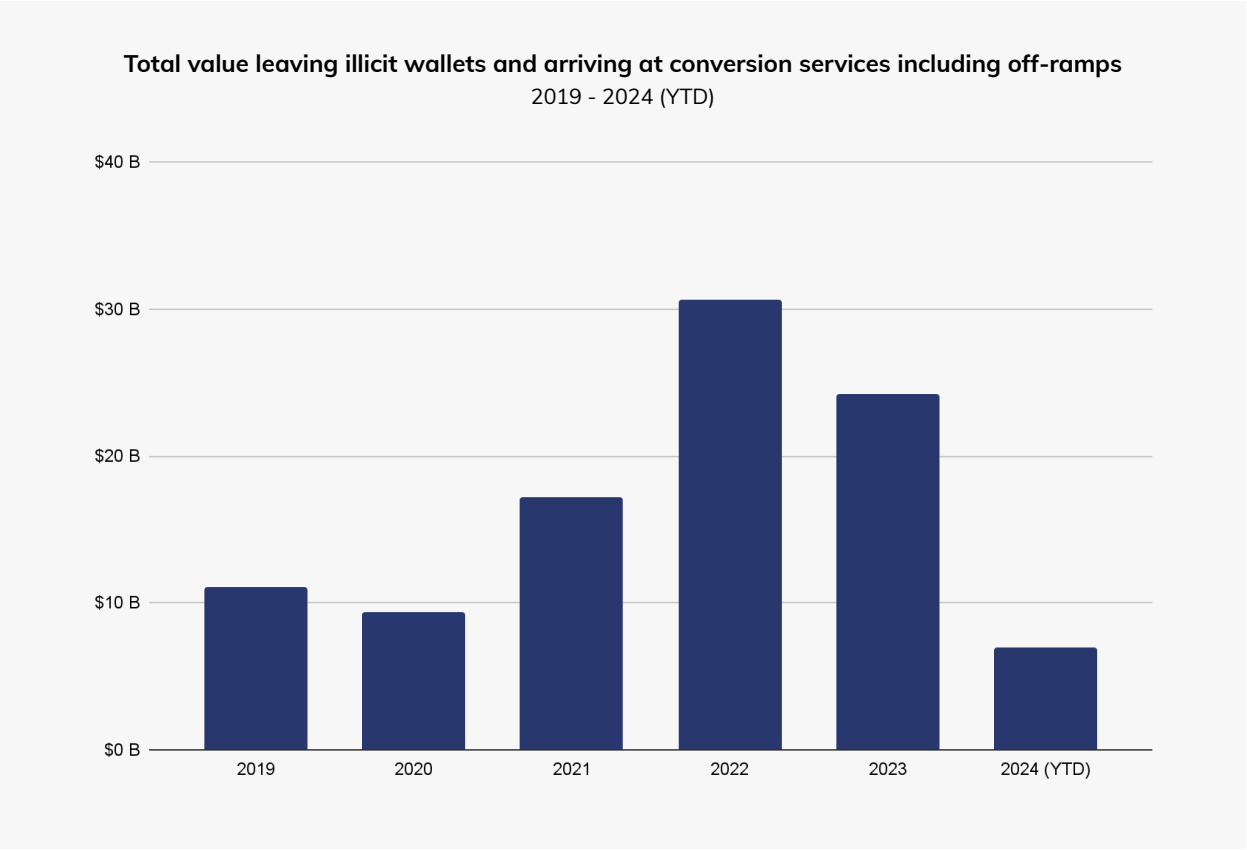
What is money laundering?

Money laundering is the process of concealing the origins of money obtained from illegal activities so that the funds can be used without drawing attention to their illicit source. This typically involves making large sums of money generated by criminal activities, such as drug trafficking or terrorist financing, appear legitimate.

The process of money laundering generally consists of three stages: placement, layering, and integration. Placement is the initial stage in which illicit money is introduced into the financial system. Layering involves moving the money through a series of financial transactions to obscure its origin. Finally, integration is the process of re-entering the money into the legitimate economy, making it appear as though it has come from a legitimate source.

Chainalysis has published money laundering analyses in our annual Crypto Crime Reports for several years, dissecting the flow of funds from known illicit wallets during the placement stage, to conversion services which represent the layering stage of laundering. Known illicit wallets hold funds connected to confirmed crypto-native criminal activity like exchange heists, crypto scams, and darknet market proceeds. Conversion services swap cryptocurrencies for fiat, other types of crypto, or provide some other service. Examples of conversion services include centralized exchanges, DeFi services, gambling sites, mixers, and bridges. Because this activity occurs entirely on-chain, we refer to it as crypto-native money laundering. This type of money laundering can be traced and analyzed with a higher degree of accuracy and speed compared to traditional financial systems thanks to the inherent transparency of blockchain.

As shown below, since 2019, nearly $100 billion in funds have been sent from known illicit wallets to conversion services. The highest amount recorded was in 2022, with $30 billion identified, largely attributable to transactions involving sanctioned services such as the Russian exchange Garantex.



These amounts represent the dollar value of the assets at the time they leave wallets associated with illicit actors. These estimates only include the totals moved from illicit sources to crypto services, and do not include the value sent and received among intermediaries – a process described below – which can include tens or hundreds of individual transactions. This estimate also does not include transactions where cryptocurrency is used to launder funds, but the source of the illicit activity is unidentified or off-chain. For example, consider a drug cartel selling narcotics and paying a distributor using cryptocurrency. If this transaction flows directly between two known exchanges, it would be indistinguishable on-chain from legitimate service-to-service transfers without specific lead information. However, investigators can still follow these funds using a combination of off-chain intelligence and on-chain analysis, and compliance teams can flag unusual transactions outside of their customers' business profiles.

In this report, we aim to broaden our analysis of money laundering to encompass not only crypto-native money laundering, but also suspicious transaction patterns that may indicate money laundering activities tied to off-chain crime that would require deeper investigation to confirm.

First, we will examine trends and behaviors within the crypto-native money laundering space, identifying key patterns and methods used by a range of threat actors. We will then explore how traditionally

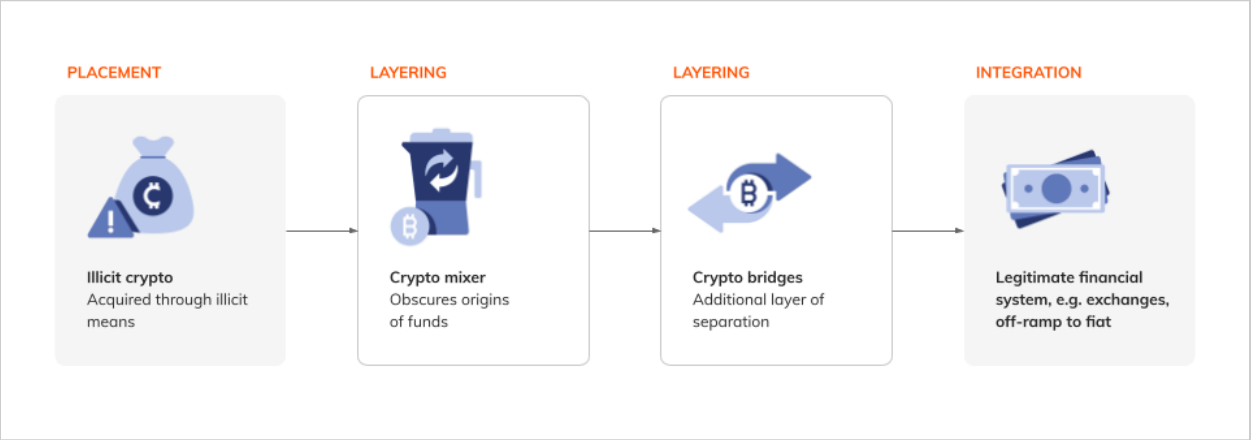
fiat-powered criminal activities are leveraging cryptocurrency for money laundering, and how blockchain analysis can provide intelligence to investigators in government and compliance.

Crypto-native money laundering

Every month, billions of dollars flow through the crypto ecosystem from illicit wallets to conversion services. Crypto-native money laundering can be particularly sophisticated, as these cybercriminals often leverage mixers, cross-chain bridges, and hops between intermediary wallets[1] to obscure the origin and movement of their funds. An advanced understanding of these mechanisms can help crypto-native actors attempt to evade detection more effectively, posing a persistent challenge for crypto services and law enforcement agencies.

We can see this complexity at play in the Atomic Wallet exploit by the North Korea-affiliated hacking group TraderTraitor in June 2023, as detailed in our 2024 Crypto Crime Report. This incident exemplifies the intricate layering involved in sophisticated crypto-native laundering, demonstrating the advanced tactics some actors use to obscure illicitly obtained funds.

On-chain laundering: A potential workflow



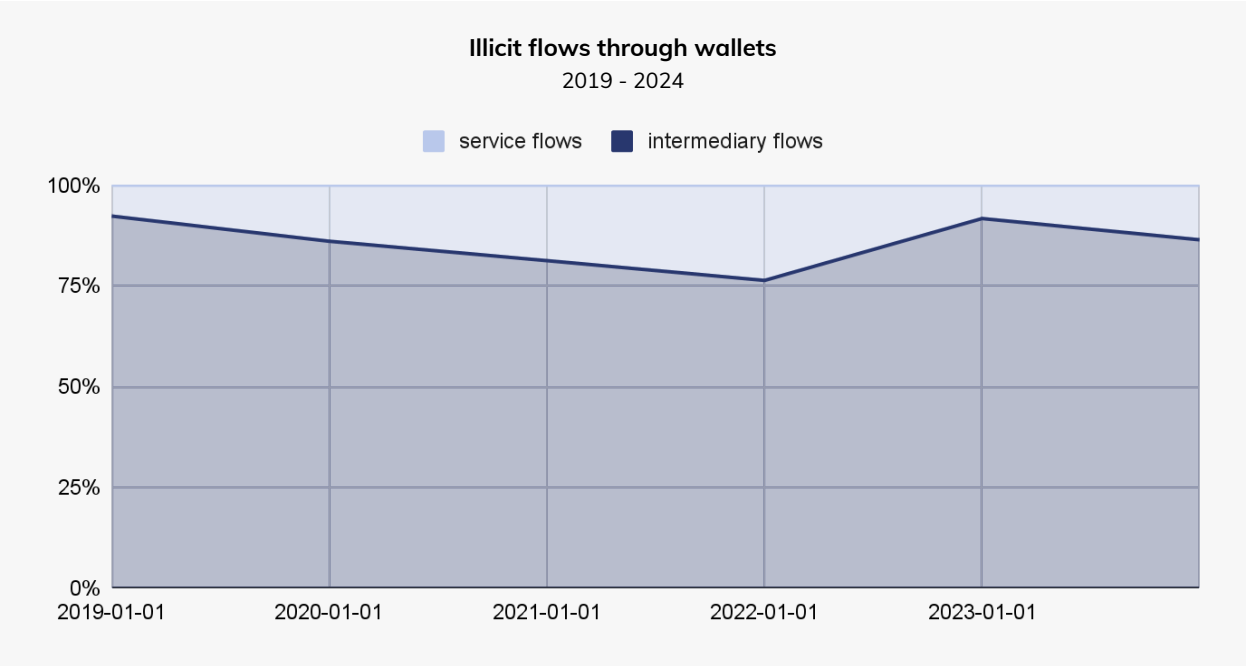
Advanced blockchain analysis technology can provide opportunities for detection and disruption throughout this process

Layering in cryptocurrency: Intermediary wallets

The layering stages of money laundering can take many forms. In traditional fiat laundering, this might involve sending funds through multiple bank accounts and shell companies. In crypto, one popular method of layering involves sending funds through numerous intermediary personal wallets — known as “hops.” This tactic is designed to obscure the connection between the illicit funds in the initial placement stage and their eventual integration.

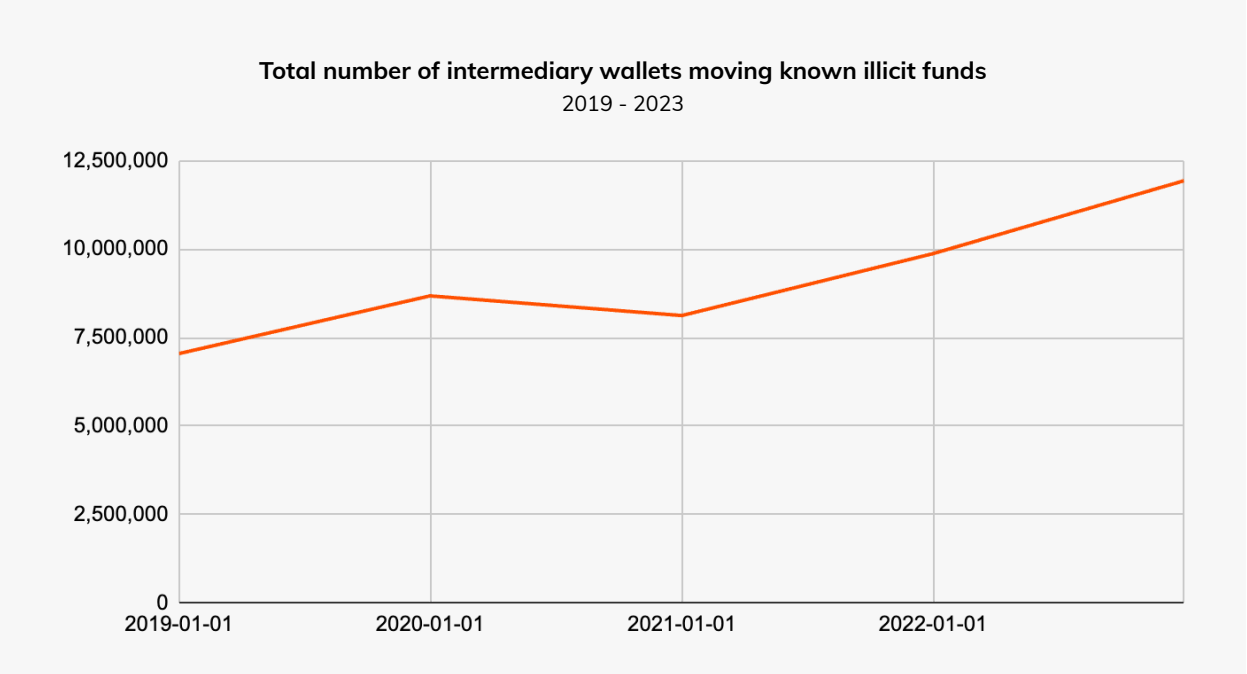
[1] From a data standpoint, we define intermediaries as distinct unidentified wallets between two known endpoints. In this money laundering analysis, intermediaries are between an illicit wallet and a conversion service. Transactions between intermediary wallets may or may not represent a change of custody. In other words, the transaction could involve a hand off from a cybercriminal to a professional money launderer, or it could be one individual sending crypto through many individual private wallets they control. In the analysis for this report, we suspect these intermediary wallets are primarily personal wallets, although they may also include unidentified services. Throughout this report, we use data science techniques to demonstrate trends in money laundering, but further investigation is required to confirm individual cases of potential money laundering.

In the on-chain laundering process, these intermediary wallets play a significant role, often accounting for over 80% of the share of the total value flowing through these laundering channels, as shown in the chart below.[2]



Additionally, growth in the number of intermediary wallets is the sort of thing we would expect if illicit actors were adding hops to their laundering process in order to increase the complexity of their operations on-chain.

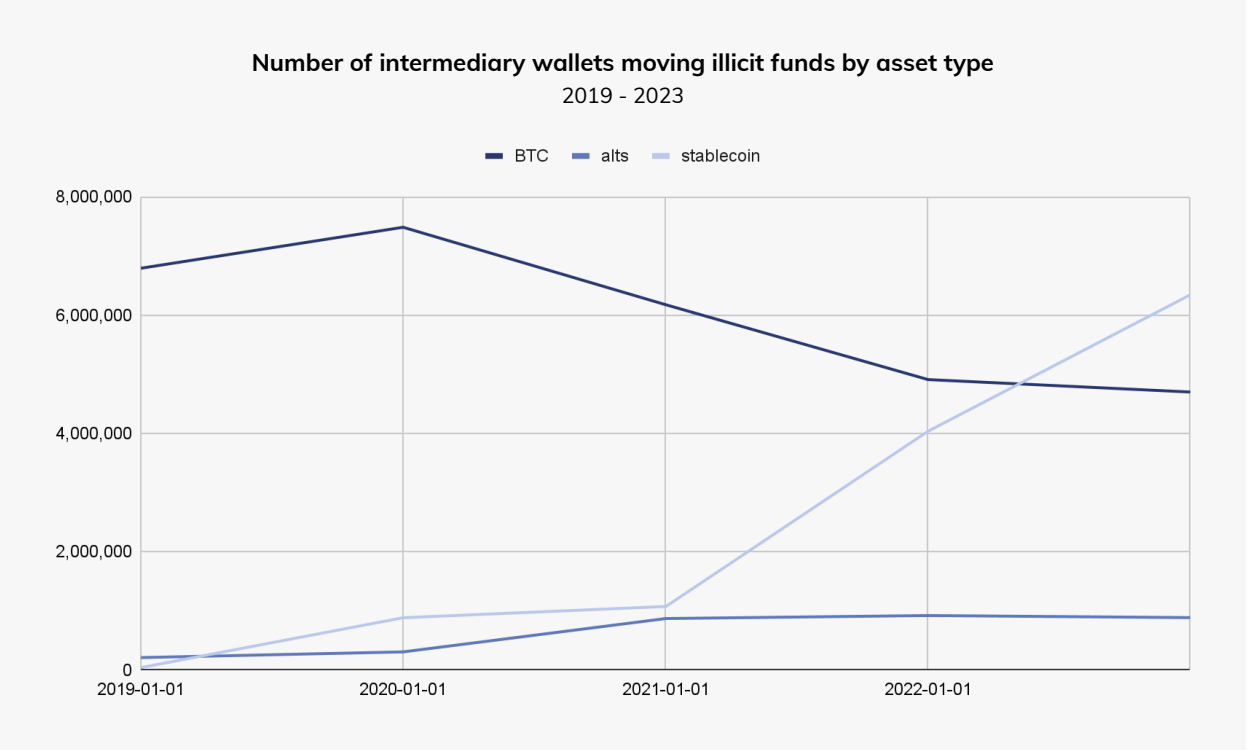
[2] "Service flows" as shown here is defined as the movement of assets from service to service, while "intermediary flows" encompasses transactions between intermediary wallets, which includes wallet-to-wallet transactions or flows from illicit wallets to intermediary wallets.



Since each hop increases the fees paid by illicit actors, these additional steps may be motivated, at least in part, by a desire to avoid detection by law enforcement and compliance teams at crypto services.

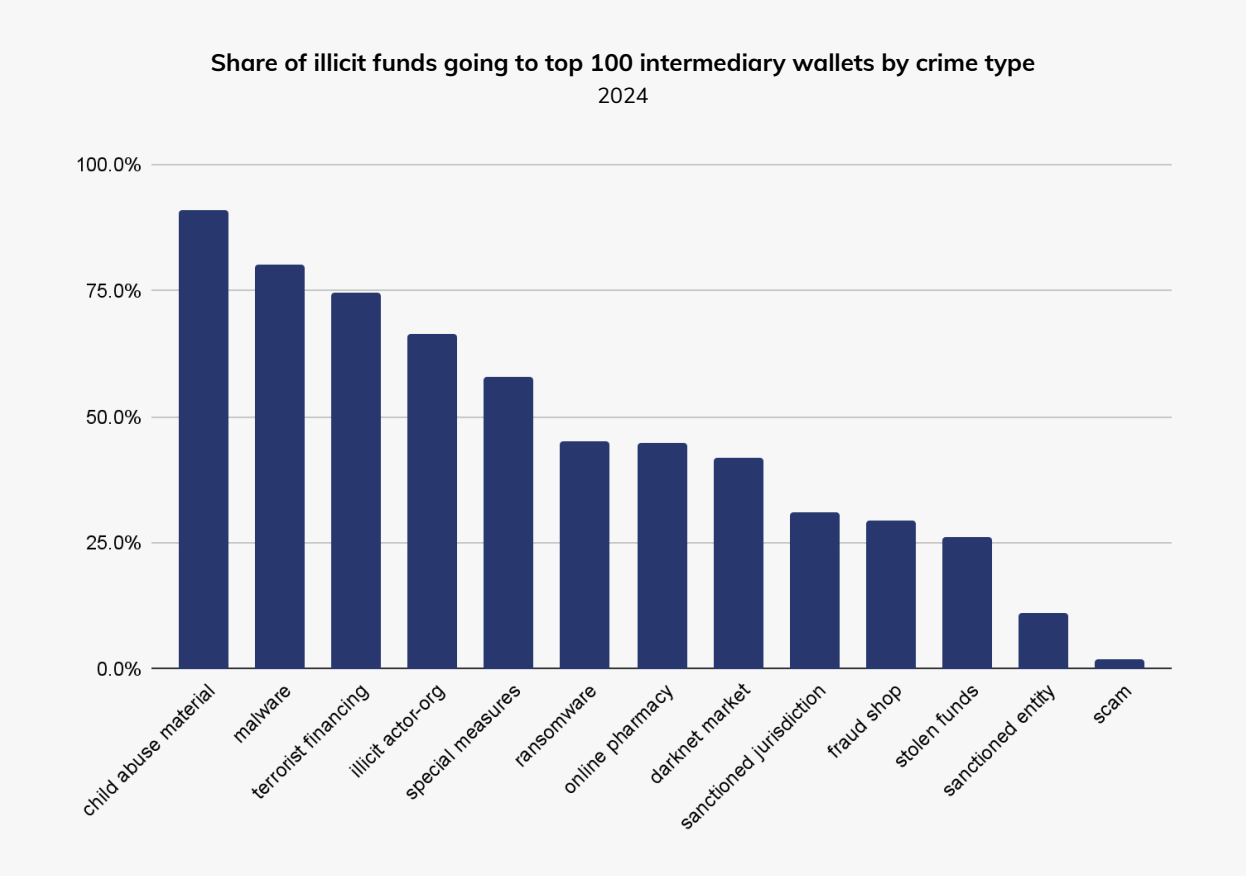
At the same time, the number of intermediary wallets between illicit wallets and conversion services typically correlates with the total amount of illicit activity we observe at a given time. For instance, the use of intermediary wallets involving illicit flows peaked in late 2022, a year we observed the most total cryptocurrency value received by illicit addresses.

An increasing portion of illicit funds passing through intermediary wallets are represented by stablecoins, consistent with our finding that stablecoins now account for the majority of all illicit transaction volume.



This rise in the use of stablecoins likely reflects the overall increase in stablecoin adoption over the last few years — after all, both good and bad actors often prefer to hold funds in an asset with a value that will not change based on swings in the market. But using stablecoins also adds an element of risk for launderers: stablecoin issuers have the ability to freeze funds, which we address later.

Data analysis can help identify intermediary wallets holding a large concentration of funds linked to crypto-native criminal activity. These wallets often act as consolidation points, holding cryptocurrency deposited from multiple other intermediary wallets.



For many crime types, only a handful of wallets hold the vast majority of illicit funds which may reflect the degree of concentration in some parts of the illicit sector.

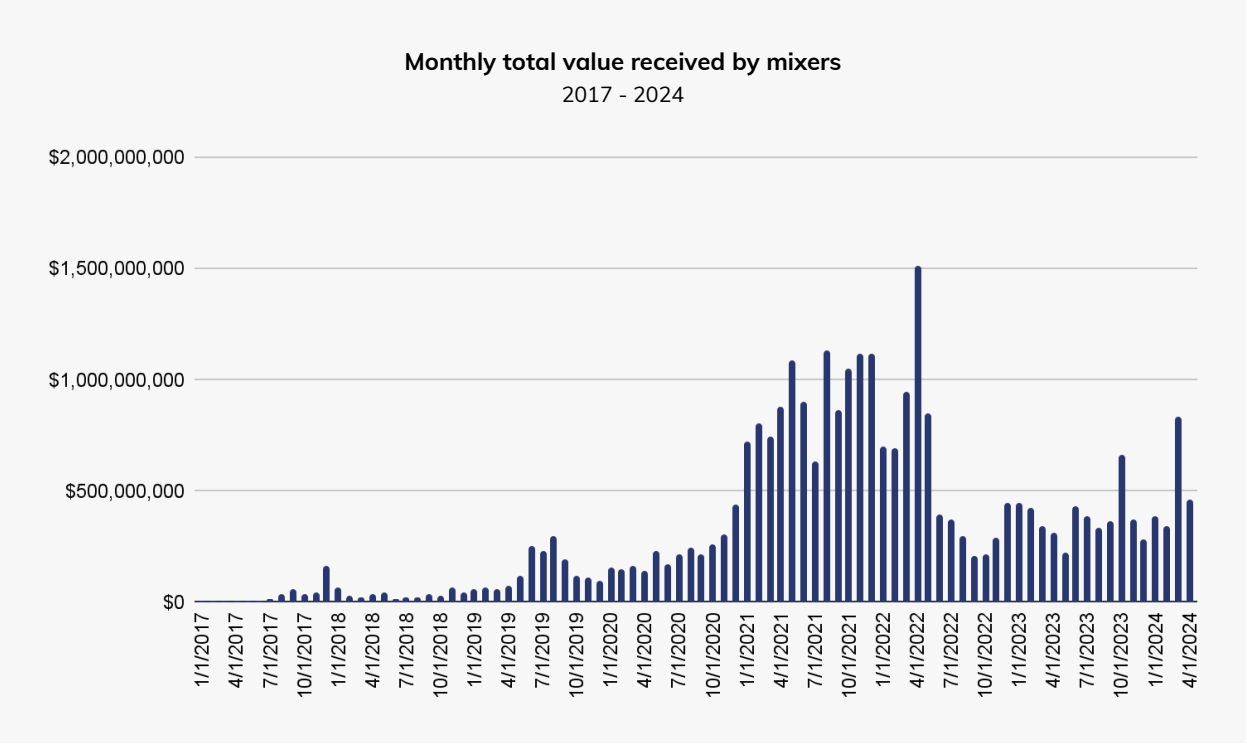
The tactic of sending funds through numerous intermediary wallets before reaching the final destination complicates the manual tracing process for investigators using block explorers. But for investigators and compliance professionals using Chainalysis, detecting illicit activity and tracing through intermediary wallets can be relatively simple.

Crypto obfuscation services

Because investigators equipped with the right tools can easily trace funds through intermediary wallets back to their illicit sources, many bad actors deploy additional obfuscation methods and specialized crypto assets in attempt to further conceal the source of funds. These tools share the common trait of breaking the on-chain link between the destination and the origin of funds, unless advanced forensics techniques are deployed. We will examine several of these obfuscation methods below.

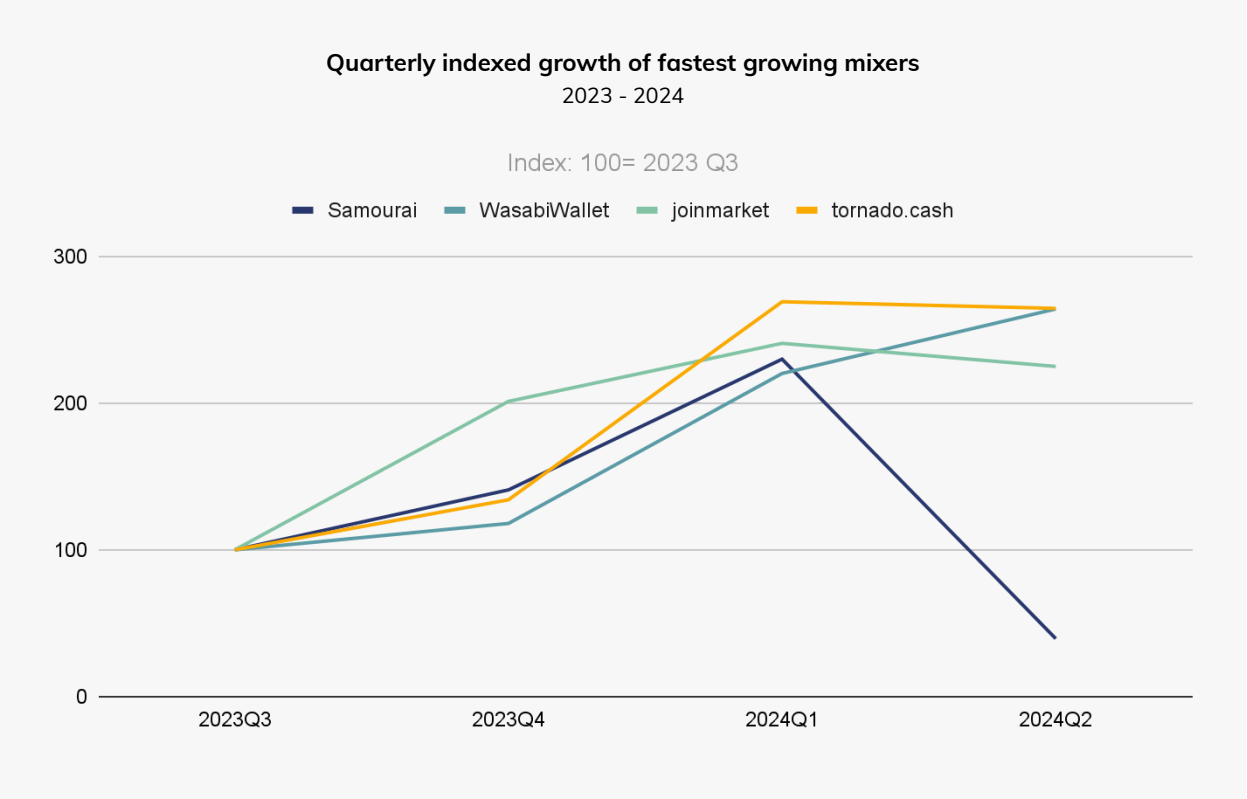
Crypto mixers

Mixers, also known as tumblers, are services that blend the cryptocurrencies of many users together to obfuscate the origins and owners of the funds. While the primary function of mixers is to enhance privacy, it is important to recognize that not all transactions processed through mixers are tied to illicit activity. In 2022, mixers reached peak popularity, exceeding $1.5 billion of value received in April of 2022.



Consistent with a general uptick in market activity, mixers have begun to see a resurgence in 2024.

When looking at the growth of individual mixing services overall, we see that WasabiWallet, JoinMarket, and Tornado Cash have grown the most.

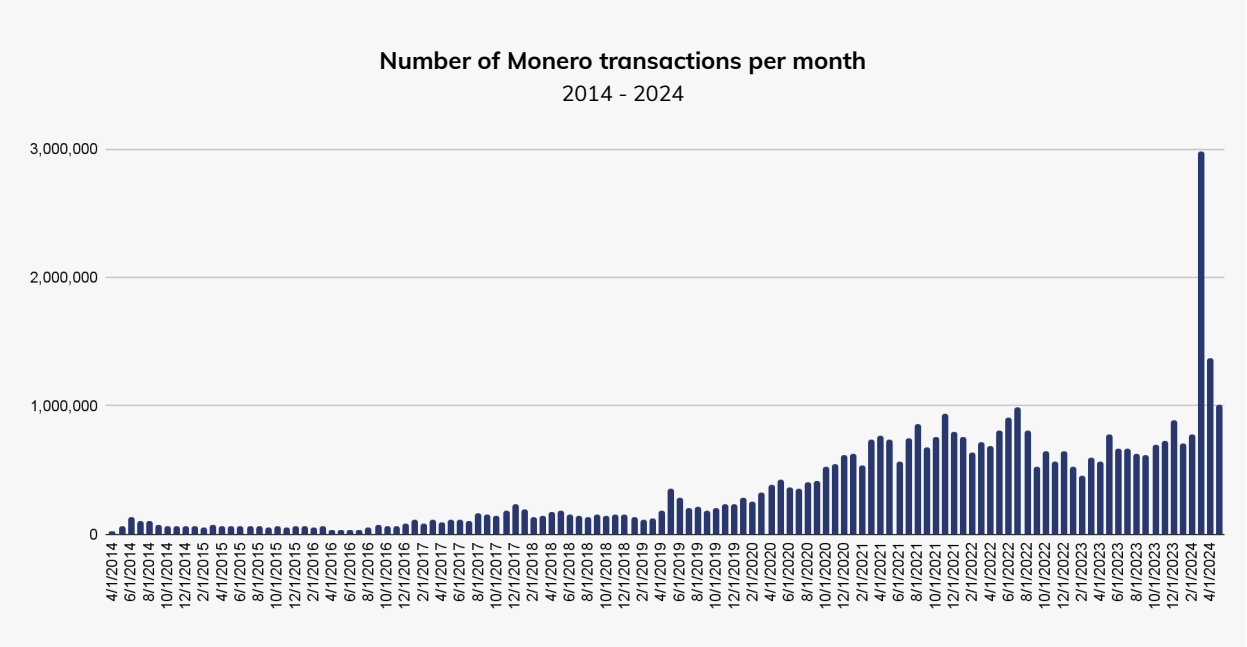


It is noteworthy that Tornado Cash in particular demonstrates sustained high growth over the past year, following a dramatic decline in usage after it was sanctioned in 2022. This is a trend we first noted in our 2024 Crypto Crime Report, where we detailed how early 2023 marked an inflection point, when inflows to the smart contract mixer began to increase again over time. Conversely, Samourai was on track to be a top performer in terms of growth this year, but that momentum has since plummeted following the April 2024 Department of Justice action against the founders and CEO.

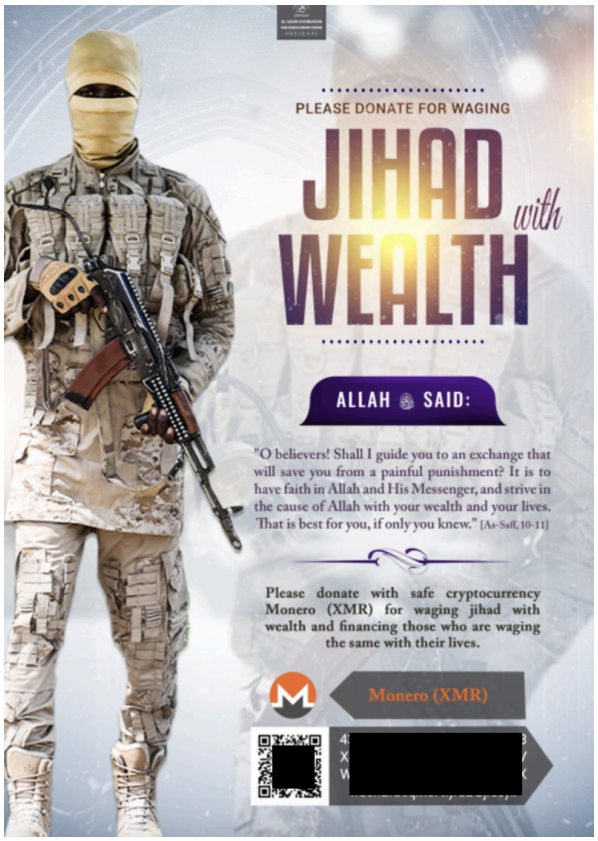
Privacy coins

Privacy coins, such as Monero (XMR) and Zcash (ZEC), offer enhanced anonymity features, making it more difficult to trace transactions on those chains. Monero uses advanced cryptographic techniques such as ring signatures, stealth addresses, and confidential transactions to obfuscate the sender, recipient, and transaction amount. As we see below, Monero transactions are on the rise overall[3].

[3] The anomalous March 2024 spike in Monero transactions can be attributed to a spam event called Black Marble.



While not all Monero transactions can be attributed to illicit activity, its privacy features may be particularly attractive to illicit actors. For example, terrorist organizations, such as the Islamic State in Khorasan's media platform, Al Azaim Media, have advertised Monero donation addresses.



Because the level of obfuscation afforded by privacy coins hides transaction details from public view, government agencies may consider investment in specialized blockchain analysis services that can make tracing Monero and other privacy coins possible.

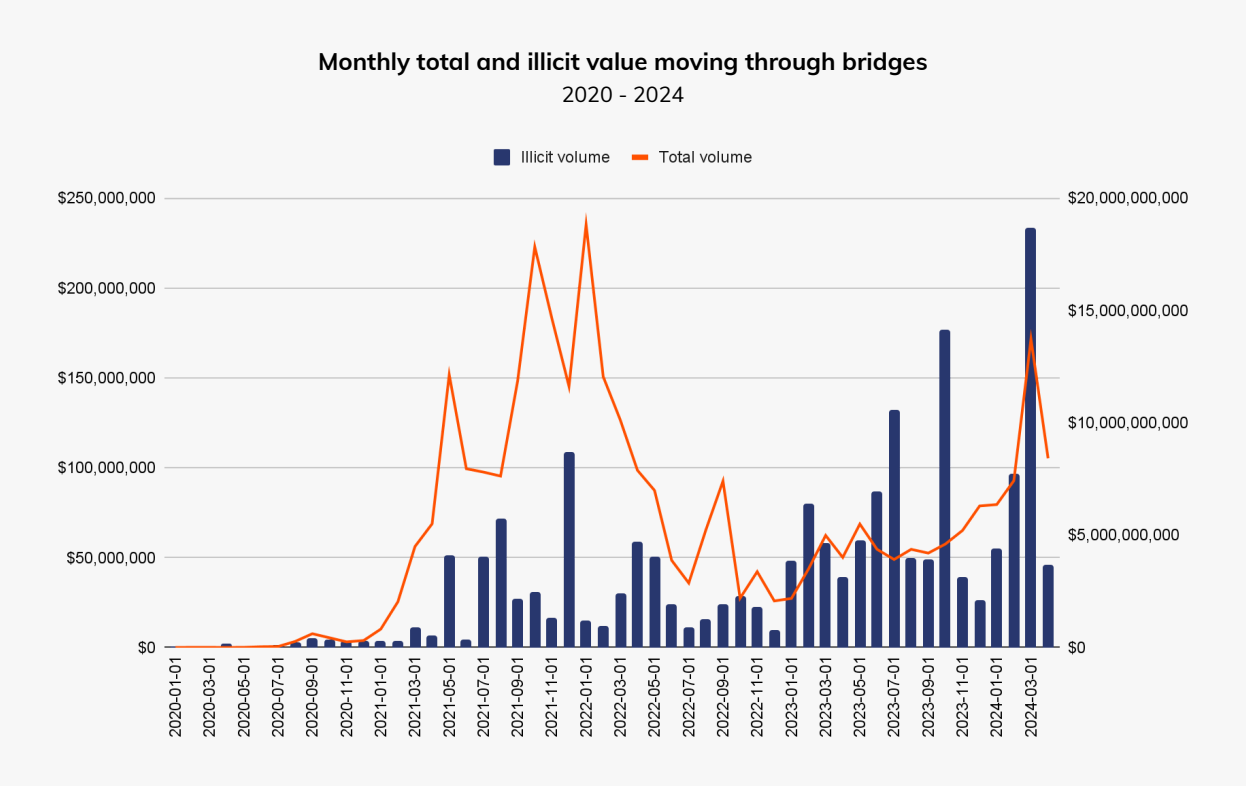
As detailed in our 2024 Crypto Crime Report, Monero's role in laundering activities is particularly evident in Monero-friendly instant exchangers, which often lack compliance measures like Know Your Customer (KYC). These exchangers facilitate the conversion of cryptocurrencies to Monero, effectively breaking the traceability chain. However, it is important to note that some regulators have banned privacy coins, and many exchanges, most recently Binance, have delisted Monero due to concerns over its potential for illicit use.

Crypto bridges

Crypto bridges, which facilitate the transfer of assets between different blockchain networks, have become popular tools that enhance the cross-chain interoperability and use cases of certain assets. As their overall usage grows, malicious actors increasingly attempt to leverage cross-chain bridges to obscure the origins of illicit funds by moving them across multiple blockchains.

Although bridge transactions can be traced by investigators with the right tools, launderers create complex webs of transactions by splitting funds into smaller amounts and transferring them across various chains, making it more time-consuming for investigators to untangle.

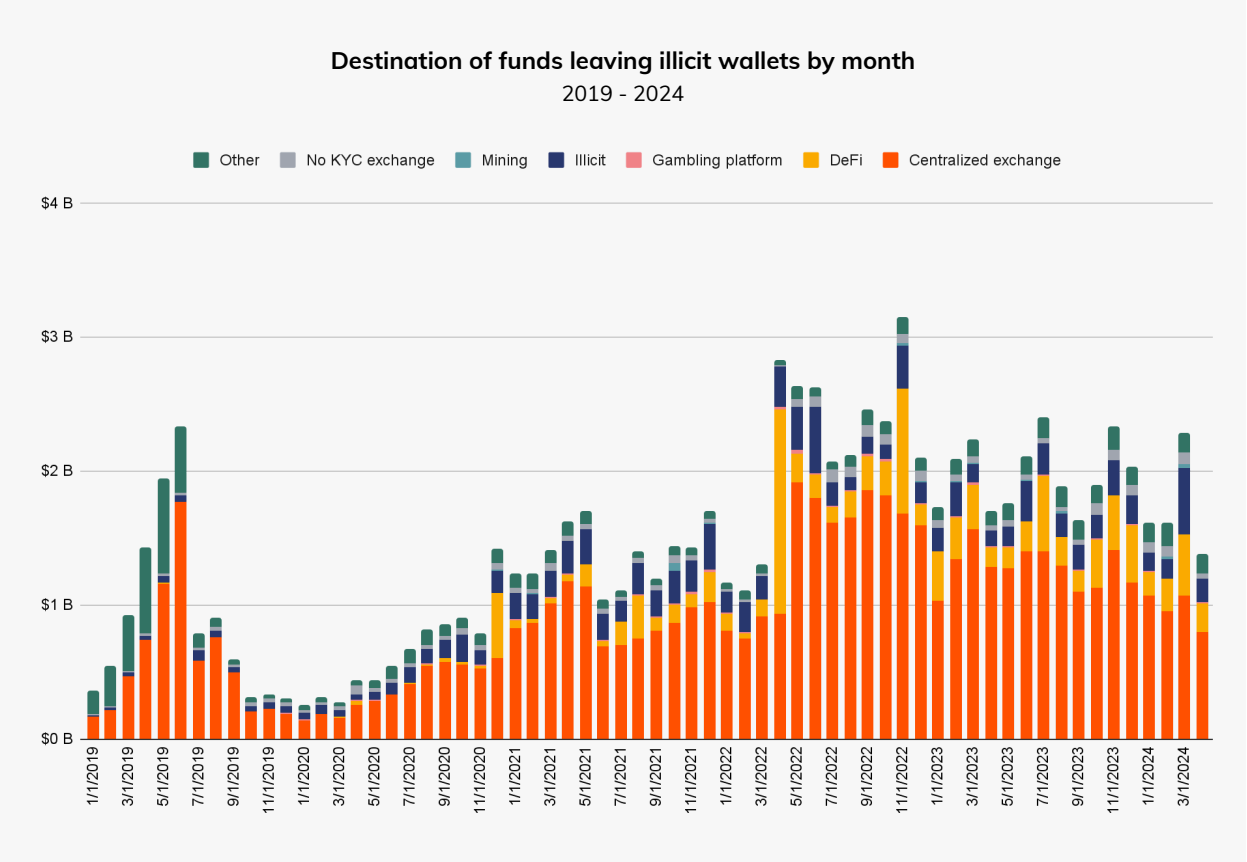
When examining illicit flows to bridges, we can see that value has increased steadily over time, continuing the trend we observed in our 2024 Crypto Crime Report.



There is a pronounced surge in illicit value starting in late 2023, with close to $234 million in illicit inflows recorded in January 2024 — the highest value to date, largely driven by funds flowing from Tornado Cash to bridges.

Destination of illicit funds

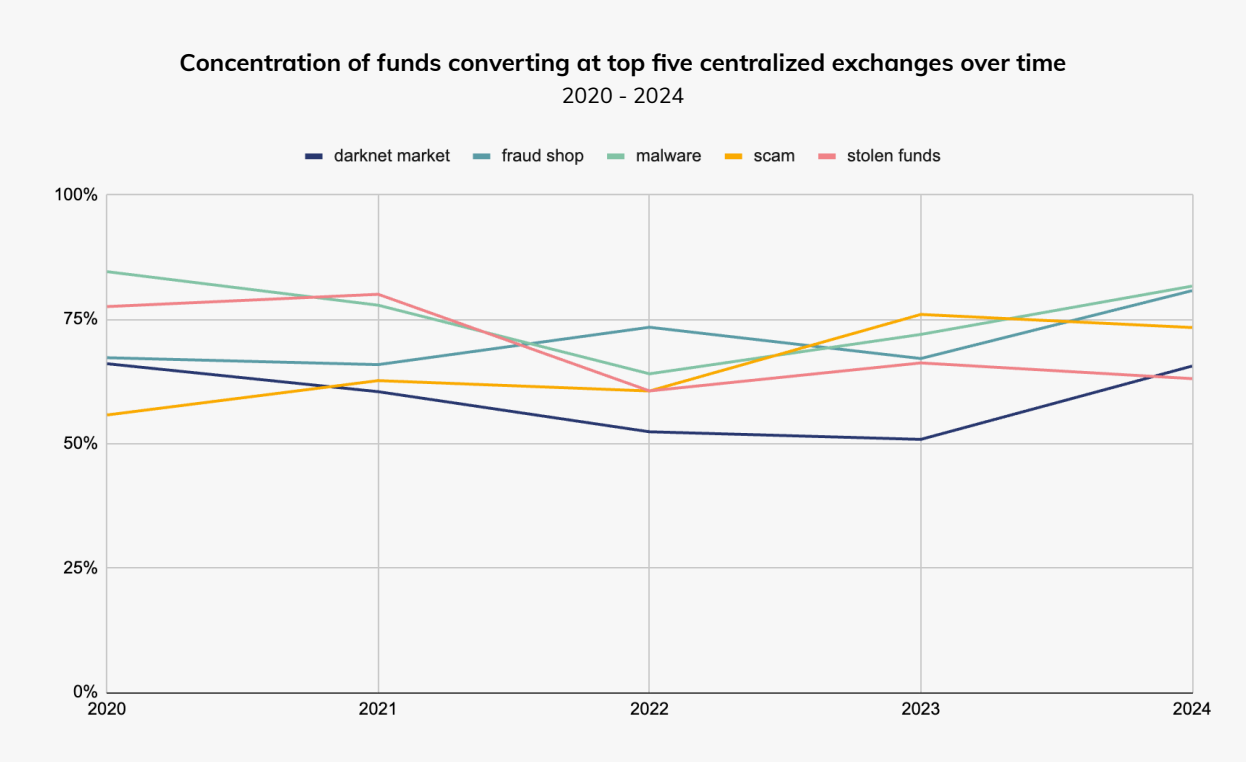
While some cybercriminals may hold their ill-gotten gains in personal wallets for years – presumably in hopes that authorities will turn their attention elsewhere – most bad actors look to off-ramp funds from crypto to cash. Over 50% of illicit funds wind up at centralized exchanges, either directly or indirectly after the use of obfuscation techniques.



Illicit actors might turn to centralized exchanges for laundering due to their high liquidity, ease of converting cryptocurrency to fiat, and integrations with traditional financial services that help blend illicit funds with legitimate activities. There are currently hundreds of centralized services in any given year that receive over $1 million in illicit funds. However, a notable downtrend in the volume received by centralized exchanges — from nearly $2 billion a month at peak to approximately $780 million a month — suggests increased efficiency in the AML programs of centralized exchanges in detecting and mitigating laundering activity.

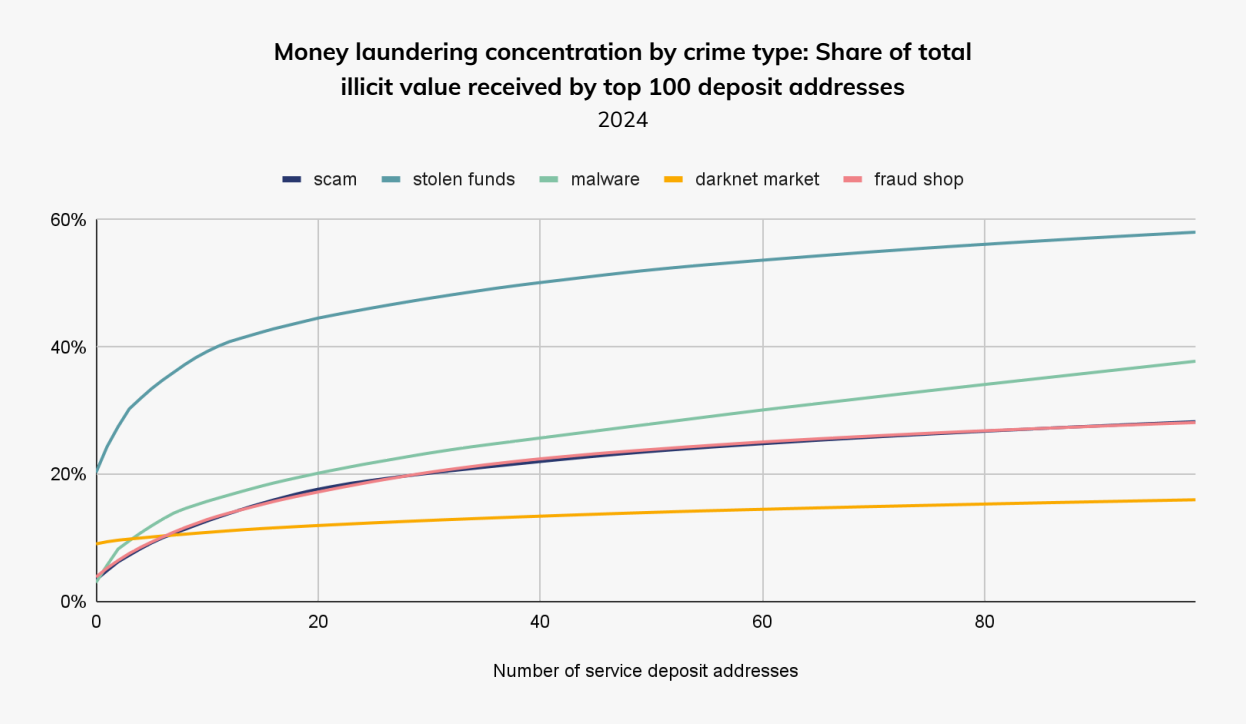
Concentration of cash-out points

Despite a dispersion across many services, there is a high concentration of illicit funds flowing to just five centralized exchanges. So far in 2024, there has been a particular surge in the use of just a few conversion services for funds from darknet markets, fraud shops, and malware.



Not only can Chainalysis analyze the types of services that are receiving illicit funds, but also the exact deposit addresses that are receiving the funds. A deposit address is similar to a bank account in that each one tends to correspond to an individual account at the service.

An interesting trend emerges when we look at the share of funds going to the top one hundred deposit addresses receiving the most illicit value in 2024. Actors attempting to cash out stolen funds tend to use fewer deposit addresses than other types of crimes, driven by a few larger outlier hacks. In contrast, revenues from darknet marketplaces show the lowest concentration among the top hundred deposit addresses, speaking to the many vendors that use them.



Still, across all categories shown above, the top hundred deposit addresses take at least 15% of all illicit funds in that category, indicating that the cybercrime community may be smaller than many suspect.

Over-the-counter brokers

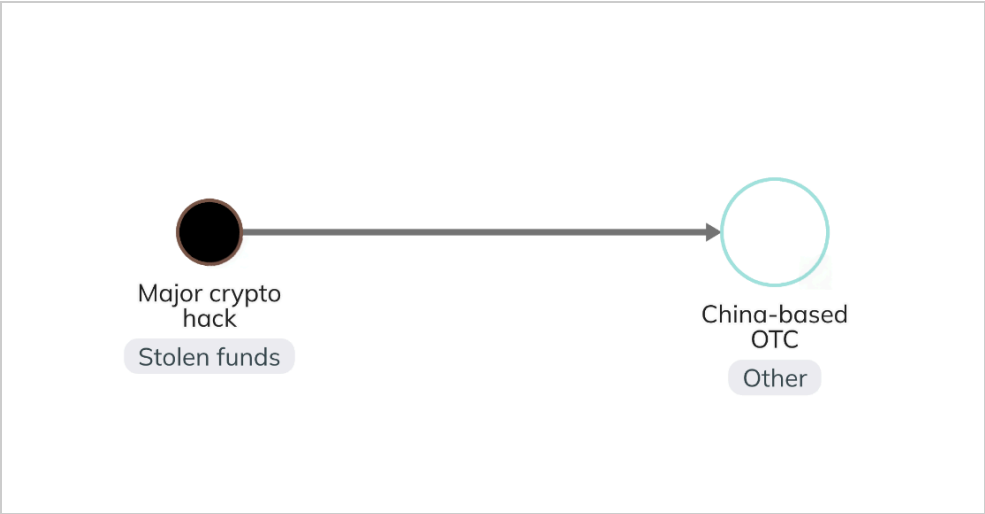
Over-the-counter (OTC) crypto brokers facilitate large trades between two parties, ensuring privacy and often better pricing for high-volume transactions. These brokers connect buyers and sellers directly through a broker-dealer network or OTC trading desks, bypassing public order books.

While most OTCs are legitimate services, there are some that have emerged that do not require proper KYC procedures for customers and oftentime specifically cater to off-ramping illicit funds. These OTCs can be found all over the world and can be difficult to identify, often requiring a combination of off-chain and on-chain intelligence.

Cybersecurity firm Cloudburst scrapes Telegram channels and looks for advertisements from these OTCs. They have recently identified many OTCs operating in China offering conversion services to fiat currency directly through Telegram channels.

Below is an example advertisement for one such OTC broker that promotes a "24-hour self-service redemption via Telegram." Their website, which advertises in Mandarin, boasts: "We have sold a large amount of USDT stolen from overseas." According to Cloudburst, this service claims to have shipped over three million USDT daily in 2024. Once a connection is established on Telegram, customers receive a deposit address digitally to facilitate transactions.

Some of these OTCs have an on-chain illicit footprint that can help profile the service in addition to the Telegram advertising. We can see another China-based OTC directly off-ramping illicit funds, as shown in the Reactor graph below.



While OTCs in general are an important part of the regulated market, certain components make them attractive to criminals, particularly when regulatory requirements are unheeded.

The crypto nexus in non-crypto native money laundering

Non-crypto native money laundering refers to the laundering of funds derived from off-chain criminal activity, rather than funds derived directly from crypto-specific crimes like hacks or scams. As more financial transactions move on-chain overall, traditional money launderers are turning to cryptocurrencies to facilitate their operations. Tracking non-crypto native money laundering can be difficult at scale outside of the context of specific investigations, as concrete evidence linking funds to illicit activity is often scarce. But below, we leverage data science techniques to examine some flags that might indicate this activity is occurring.

Typologies of suspicious on-chain activity and examples of heuristics that can help identify them

The relationship of traditional money laundering methods with blockchain has expanded the toolkit available to money launderers – and their tracers. Monitoring financial flows for suspicious activity which often relies on heuristics and thresholds, such as in the Financial Action Task Force (FATF)'s Red Flag guidance to describe behavior that could be suspicious. Additionally, guidance from the Financial Crimes Enforcement Network (FinCEN) suggests that potential money laundering and sanctions evasion related to Russia can be signaled by unexplained surges in value flows and other unusual transactional patterns.

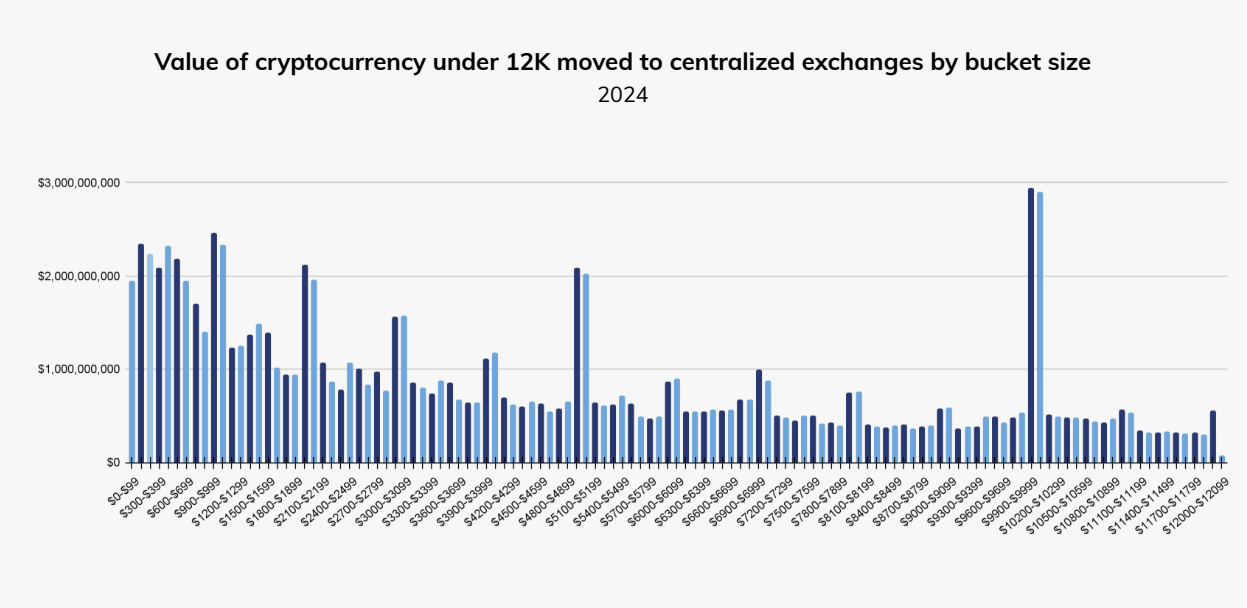
The use of blockchain data-driven heuristics can augment the existing workflows of compliance teams and investigators to help identify potentially suspicious on-chain activity. It is important to note in all of these cases that the patterns identified are not, in isolation, a confirmation of wrongdoing.

Repeated transfers just under reporting thresholds

While the threshold varies by country, FATF recommends that cryptocurrency transactions exceeding $1,000 USD/EUR be subject to the Travel Rule, with the United States (U.S.) setting this value at $3,000 USD. Additionally, the U.S. Bank Secrecy Act (BSA) requires reporting on cash transactions exceeding $10,000 USD.

Transactions in excess of these values trigger additional scrutiny, while transactions under these thresholds, even by just a dollar, do not face the same level of inspection.

The chart below displays the value of funds moving to centralized exchanges by transfer size for 2024 year-to-date. It reveals a noticeable surge in transfers just below the $1,000, $3,000, and $10,000 thresholds, as well as just above it. The transfers slightly above these thresholds could potentially be attributed to rounding differences in exchange rates. The surges are typical patterns that are identified when bad actors are structuring payments to avoid triggering reporting requirements. Transactions just below reporting requirements is one of the red flag indicators FATF has highlighted for in guidance for Virtual Asset Service Providers (VASPs) to help identify suspicious behavior.



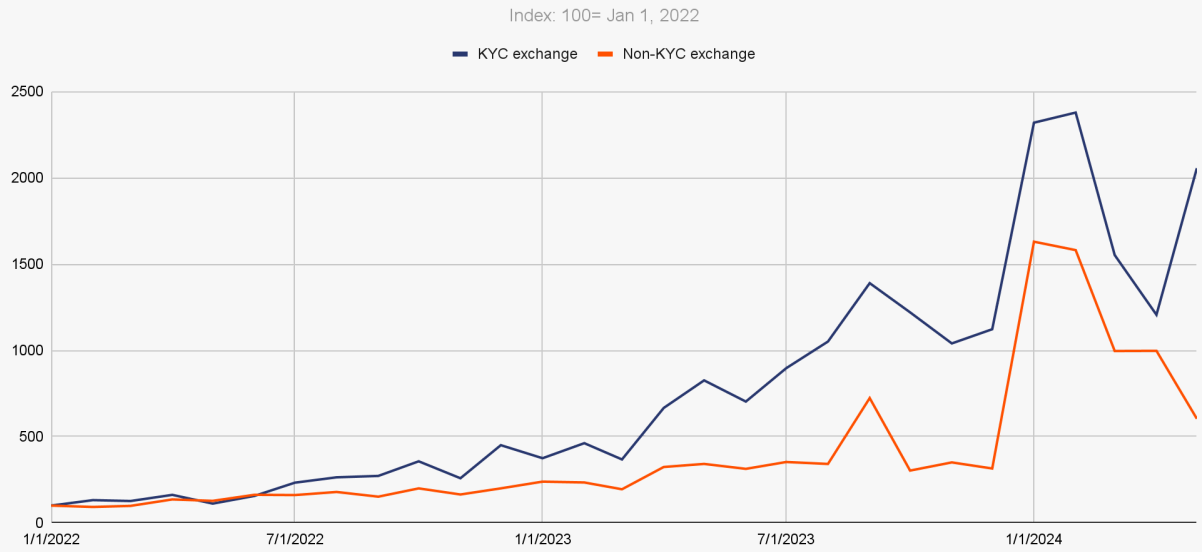
This suggests that reporting requirements are likely to increase activity at the margins, just below and slightly above the reporting thresholds, in an attempt to avoid triggering additional scrutiny.

Use of many intermediary wallets ahead of cash-outs

As discussed above, one popular method of layering in crypto-native money laundering involves sending funds through many intermediary personal wallets. Of course, the use of personal wallets is not inherently suspicious, but we can use data to answer questions about potentially suspicious behavior.

For example: Do users send funds through more intermediary wallets before converting funds at exchanges that have KYC verification versus those that do not?

Indexed monthly growth of intermediary wallets used to move illicit funds at KYC vs. non-KYC exchanges
2022 - 2024



They do. The above chart illustrates that the number of intermediary wallets used by bad actors is growing faster on KYC exchanges when compared to non-KYC exchanges. This may suggest that awareness of AML/KYC obligations might be prompting this greater use of intermediary wallets in attempts to avoid the detection of illicit activity. Although there are many legitimate reasons for funds to pass through multiple wallets, exchanges might consider the number of intermediary wallets as a potential red flag indicator as part of their overall risk assessment of a user.

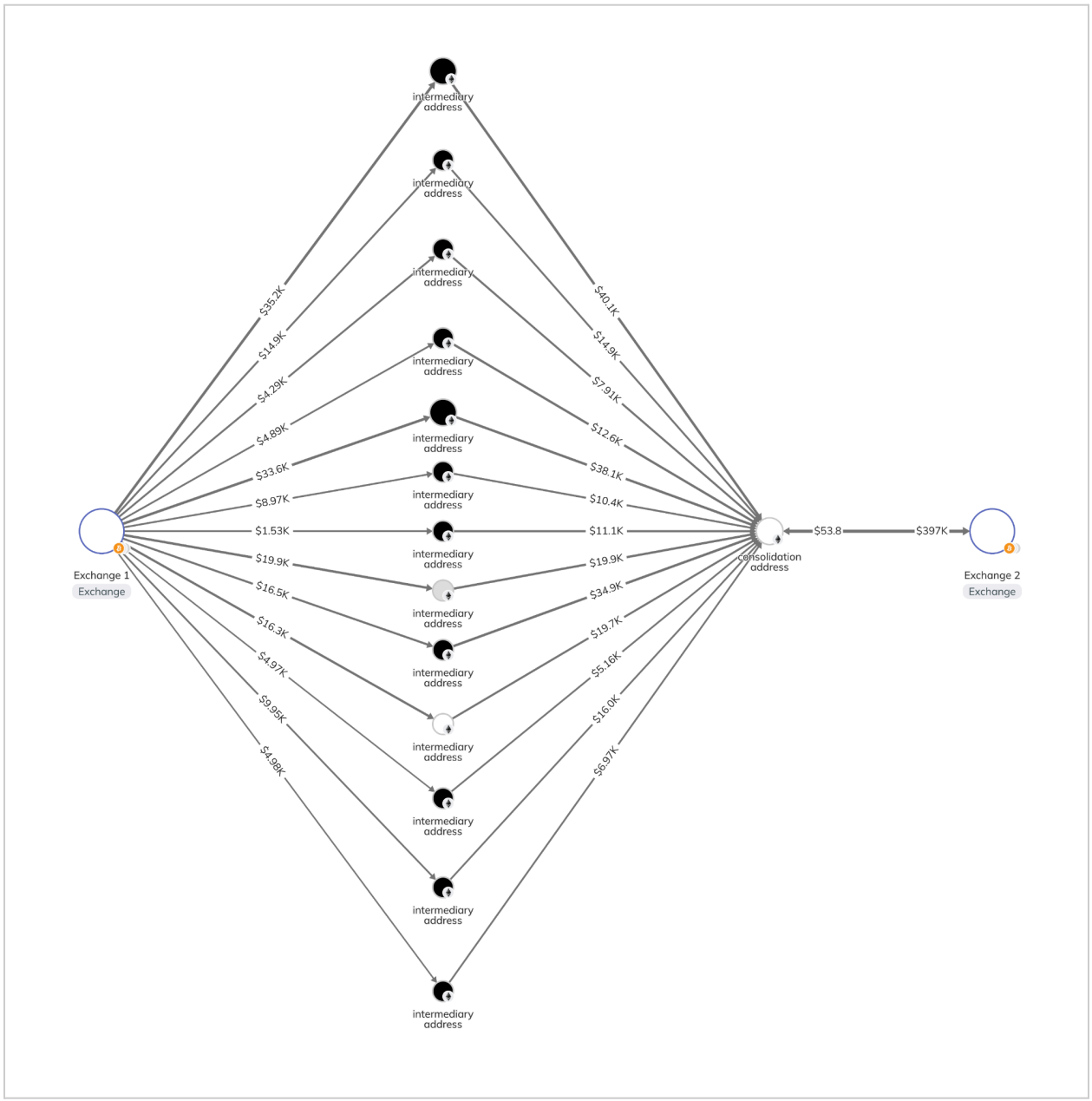
Use of consolidation wallets

Exchanges might also benefit from monitoring consolidation wallets that interact with their service. When launderers layer funds through many intermediary wallets, the transaction flows are often not simple and linear. Rather, the launderer might split funds off into many wallets and then reconsolidate the funds later, after multiple transactions.

A consolidation wallet receives and combines funds from several wallets or sources. If funds move through multiple separate intermediary wallets and then consolidate at a single address, this might suggest an attempt to avoid detection.

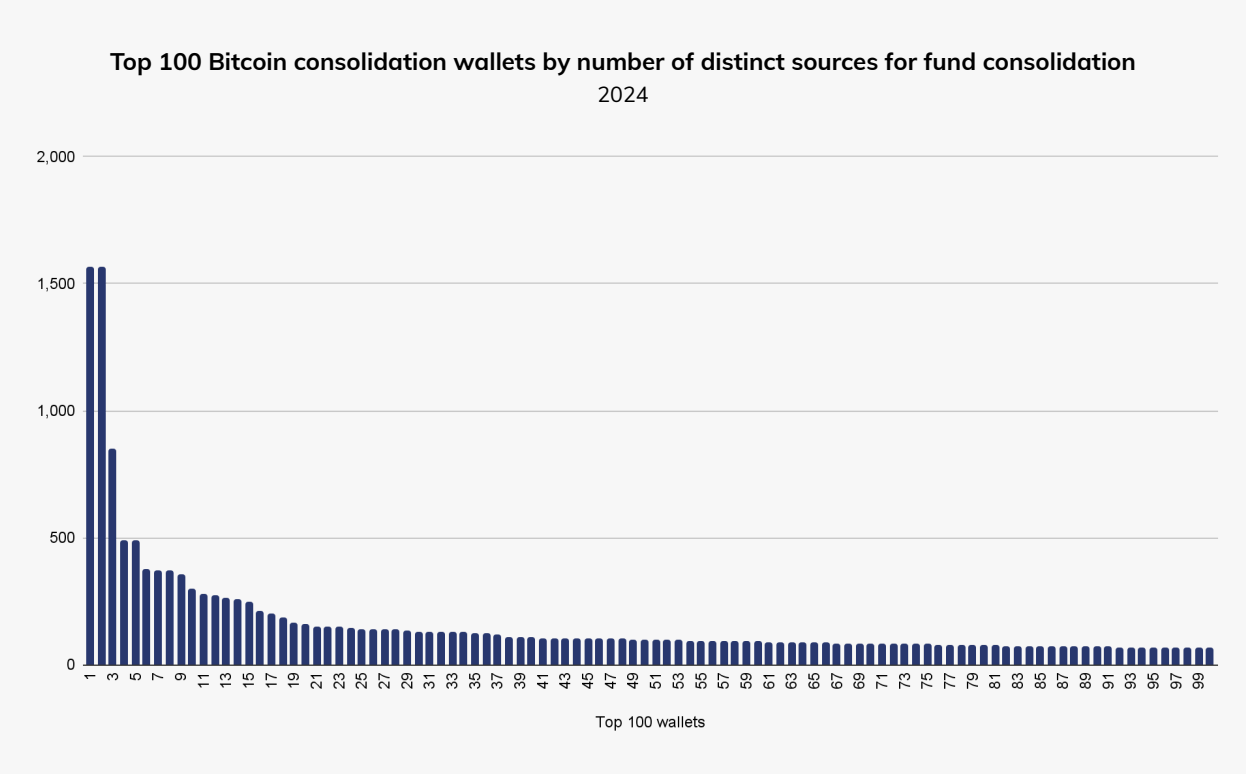
The Chainalysis Crypto Investigations graph below demonstrates this type of behavior in a known scam group targeting the elderly. In this scenario, the scammer likely instructed their victims to use a specific service, Exchange 1, to purchase crypto assets. Each victim was then directed to send funds to a different

wallet controlled by the scammer. The scammer subsequently consolidated these funds into a single wallet before cashing out at Exchange 2.



Compliance teams at Exchange 1 would have difficulty directly linking the victims to the scammer, especially if the intermediary addresses are single-use with no prior ties to illicit activity — unless they traced the transactions to the consolidation wallet. The use of many intermediaries prior to consolidation is a strategy to prevent the compliance team at Exchange 1 from understanding the connection between all the victims that were sending funds.

While the example above is relatively simple, more complex money laundering networks feature consolidation wallets that aggregate funds from dozens or even hundreds of intermediary wallets. Querying Chainalysis data can point investigators to major consolidation wallets, which may serve as useful leads. For example, this year so far, the top one hundred bitcoin consolidation wallets in 2024 – all of which have transacted two hops away from an exchange – received $968 million worth of bitcoin from over 14,970 distinct addresses.



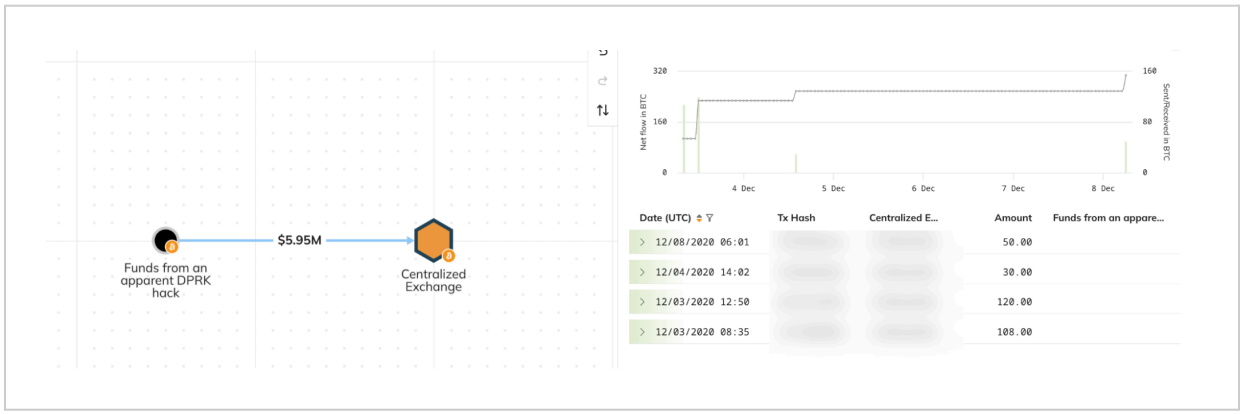
Further expanding the aperture, we can identify over 1,500 consolidation wallets that have received a total of $2.6 billion worth of bitcoin in 2024; each of those have received funds from at least ten different wallets. Again, we cannot say for certain that this represents money laundering activity – in fact, much of it likely represents legitimate economic flows. But this activity may warrant additional scrutiny.

Payments made in rounded amounts

There are many legitimate reasons why cryptocurrency users might frequently transfer rounded amounts to conversion services. For instance, people often strive to become a “whole coiner” or attain a rounded number in a given asset for psychological reasons.

Nevertheless, it is important to consider how rounded payment amounts are often found in the money laundering patterns of known illicit actors. For instance, in the laundering activities of actors linked to the Democratic People’s Republic of Korea (DPRK), launderers are known to break a large amount of funds into smaller, rounded amounts and send these at high frequencies to conversion services. Below we see that

actors suspected to be affiliated with DPRK sent four transactions totaling 308 BTC in rounded amounts to a deposit address on a centralized exchange over four days, presumably to off-ramp into fiat.



Chainalysis data shows that most personal wallets engage in transfers of rounded amounts only three to five times. Notably, only thirty three personal wallets have sent more than a thousand rounded amounts to a deposit address. That behavior may be indicative of methodical, professional money laundering or of a service that pays out in rounded amounts, prompting deeper investigation.

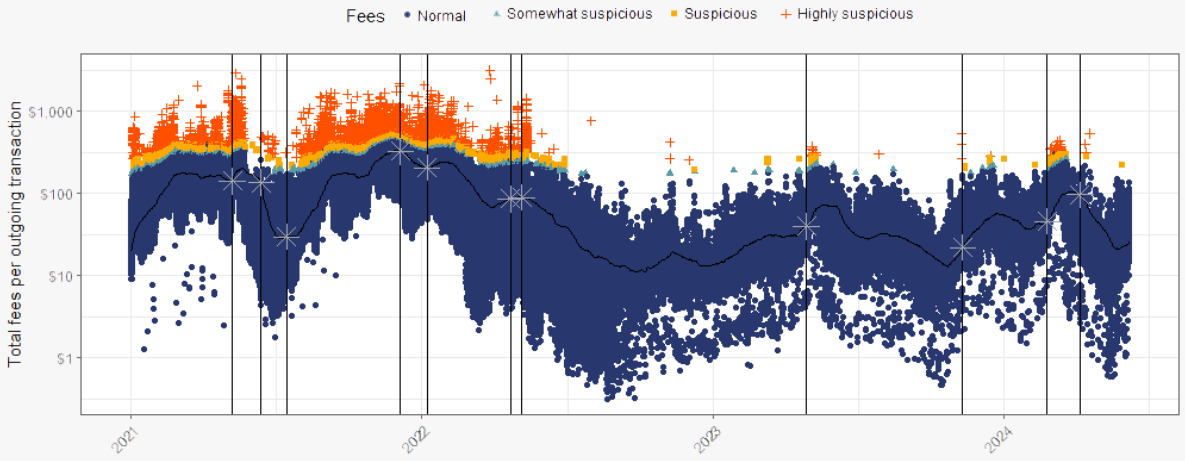
A potential reason for sending rounded amounts is that it is easier to find buyers at P2P exchanges, OTCs (over-the-counter brokers), or other informal services when dealing with whole units. For illicit actors looking to cash out, time is often more critical than obtaining the best price, making speed a higher priority at this stage of the laundering process. Regardless of the intention, investigators often flag many rounded amounts in an investigation as a noteworthy pattern.

Suspiciously large fees using mixers

As discussed above, services like mixers are designed to obfuscate the trail between origin and destination points. However, the detailed record of on-chain events can still help identify suspicious activity.

The chart below shows transaction fees from the sanctioned smart contract mixer Tornado Cash. By examining the 30-day moving average of fees, we can identify whether a transaction pays an abnormally large fee. For example, if the average fee over the past 30 days is $1, a fee of $100 would be anomalously large, while a fee of $1.01 would not. At the same time, paying $1.01 might be anomalous if fees are ranging around 10 cents.

Anomalously large Tornado Cash outgoing fees associated with stolen fund inflows to the mixer



This method clearly categorizes transactions that prioritize speed (via higher fees) over economic efficiency. While transactions with anomalously high fees are not necessarily illicit or indicative of money laundering, it is notable that significant fee surges often coincide with inflows to Tornado Cash from wallets holding stolen funds (indicated by the black lines in the chart, each representing a date of a prominent hack or theft). Analyzing fees might suggest efforts to quickly clear funds, potentially facilitating the laundering process and advancing it from the layering to the integration phase.

Applying traditional money laundering detection techniques to the blockchain

In many ways, identifying novel on-chain patterns that might indicate laundering is similar to detecting these activities in fiat currency, where the focus is on analyzing transaction patterns and anomalous activities. Conventional money launderers are onboarding to crypto, with methods that resemble their fiat-based strategies. While distinguishing between money laundering and legitimate transactions on-chain can be challenging, the insights from blockchain intelligence tools like Chainalysis are more powerful due to the transparent and immutable nature of blockchain. Traditional finance (TradFi) relies heavily on compliance procedures to trace the sources of funds, whereas blockchain offers clear visibility. Despite this, malicious actors are applying traditional laundering techniques to blockchain ecosystems in order to attempt to evade detection. As the global acceptance of cryptocurrencies grows and barriers to entry diminish, Chainalysis expects this type of money laundering to become more significant, as illicit actors historically co-opt new technologies for their own purposes.

Authorities must navigate the usage of these heuristics carefully, ensuring they have robust evidence to support their claims without unduly disrupting legitimate financial operations.

Anti-money laundering (AML): Policy and prevention strategies

Effective prevention of money laundering in both crypto native and non-crypto native scenarios requires a multifaceted approach. This includes regulatory measures, technological innovations, and global cooperation. Strategies must be tailored to address the unique characteristics of cryptocurrencies while reinforcing traditional anti-money laundering (AML) measures.

Overview of existing regulations

As crypto assets enter the mainstream, countries across the world have steadily introduced regulations addressing various properties of cryptocurrency, including anti-money laundering (AML) and Countering the Financing of Terrorism (CFT) measures, counter proliferation financing (CPF), consumer protection measures, market conduct policies, and prudential requirements. To that end, the intergovernmental Financial Action Task Force (FATF) has issued guidance laying out a comprehensive framework for countries to implement in order to combat money laundering activities.

Anti-money laundering (AML) requirements

AML requirements, including Know Your Customer (KYC) rules, are foundational regulations requiring financial institutions, including VASPs, to take a number of measures to prevent money laundering. This includes verifying the identities of their customers and monitoring their transactions for suspicious activity.

Travel Rule

The Travel Rule mandates that financial institutions, including VASPs, obtain, and in many cases, also share information about the originator and beneficiary of transactions over a certain threshold, ensuring transparency and traceability.

While public blockchains provide unparalleled visibility into transaction flows, their pseudonymous nature necessitates a different approach to abide by the Travel Rule. To this end, regulatory technologies — such as Chainalysis' partnership with Notabene and VerifyVAS — are allowing VASPs to enhance their compliance strategies.

Stablecoin issuers and freezing capabilities

Most stablecoins, such as USDT (Tether) and USDC (USD Coin), are issued by centralized entities that have the authority to control and manage their smart contracts. As such, these issuers can proactively monitor transactions for suspicious activity and freeze funds when necessary. This capability allows issuers to swiftly respond to law enforcement requests.

For instance, both Tether (USDT) and Circle (USDC) have previously indicated that they have frozen addresses associated with illicit activities. Tether tells Chainalysis that they have frozen an estimated 1,600 addresses holding funds worth approximately 1,500,000,000 USDT.

Leading regulatory frameworks

In 2019, the intergovernmental Financial Action Task Force (FATF) issued detailed guidance on the application of AML/CFT standards in the virtual asset sector for combating illicit financial activities. Since then, regulators worldwide have been working to incorporate FATF's global standards into their own regulatory frameworks, in effort to achieve a cohesive and unified approach to digital asset AML regulation on a global scale.

European Union

In 2018, the European Union (EU) adopted the Fifth Anti-Money Laundering Directive (5AMLD), to combat money laundering and terrorism financing related to digital assets. This directive required national transposition by EU Member States and came into effect in January 2020, extending AML requirements to VASPs. Additionally, the existing Transfer of Funds Regulation (TFR) — the EU's implementation of the Travel Rule — has been updated to also include crypto asset transactions by VASPs, effective December 2024, alongside the provisions for crypto-asset service providers under the Markets in Crypto-Asset Regulation (MiCA).

- 5AMLD requires greater transparency in financial and crypto asset transactions and beneficial ownership information. VASPs must conduct enhanced due diligence on high-risk customers and transactions, including identifying and verifying the identities of clients involved in complex or large scale transactions. It also encourages cooperation and information sharing between Member States and financial intelligence units (FIUs) to effectively combat money laundering and terrorist financing on a broader scale.
- TFR requires financial institutions, including VASPs, to obtain and partly verify information on originator and beneficiary and — when transacting with another VASP — transfer this information in advance of, or simultaneously, with sending a crypto asset transaction. Receiving VASPs must verify the accuracy of the information received before making crypto assets available to customers.
- In 2023, to further harmonize the approach to AML supervision among EU Member States, the EU has also adopted a set of three new AML regulations, collectively known as the "AML package."
    - Anti-Money Laundering Regulation (AMLR): Replacing parts of 5AMLD, AMLR introduces the EU's first "single AML rulebook" for obliged entities, applicable from July 2027.
    - Anti-Money Laundering Regulation Authority (AMLAR): Establishes the EU's first supranational AML Authority (AMLA) to harmonize supervision of obliged entities in the EU. AMLA is expected to be working on EU-wide policies from 2025, and directly supervising firms from 2028.
    - Anti-Money Laundering Directive 6 (6AMLD): Repeals 5AMLD directs EU Member States to implement changes into national laws within three years, focusing on the organization of national AML/CFT supervision, such as financial intelligence units (FIU.)

Singapore

Singapore is known for its robust regulatory framework. The Monetary Authority of Singapore (MAS) administers the AML/CFT regulatory regime for financial institutions, including crypto businesses. .

- Crypto businesses operating in Singapore (known locally as digital payment token service providers) are regulated under the Payment Services Act (PSA), which first came into effect in

January 2020. AML/CFT requirements for crypto businesses are set out in MAS Notice PSN02, and are supplemented by detailed guidance.

- MAS continues to enhance its regulatory framework for crypto businesses, most recently expanding the scope of regulation by bringing into force the Payment Services (Amendment) Act 2021. This Act expanded the range of crypto businesses subject to AML/CFT and other regulation to cover custodial service providers, as well as businesses facilitating the transmission or exchange of crypto, even where the latter does not come into possession of customer assets.
- Singapore recently published an updated National Money Laundering Risk Assessment as it prepares for its upcoming FATF Mutual Evaluation.

Hong Kong

Hong Kong authorities are known for their thorough supervision across different risk areas, including AML/CFT. In Hong Kong, the Securities and Futures Commission (SFC) is the primary regulator for virtual asset trading platforms (VATPs), while the Hong Kong Monetary Authority oversees the activities of banks and will eventually oversee stablecoin issuers.

- In December 2022, Hong Kong's Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) was amended to formally cover the operation of virtual asset businesses. The new regulatory regime for VATPs came into force on 1 June 2023.
- Strict and granular AML/CFT requirements for VATPs are set out in a standalone chapter of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism for Licensed Corporations. The guidelines include lists of red flags and indicators of money laundering risk or suspicious activities.
- In addition, in February 2024, Hong Kong authorities issued proposals for the regulation of OTC crypto service providers. Under the proposals, OTC platforms would need to be licensed by the Customs and Excise Department and would need to comply with AML/CFT obligations.

The United Kingdom

The UK has taken proactive steps to disrupt money laundering operations with proactive national enforcement measures and a strong emphasis on educating businesses and the public about AML risks and compliance obligations.

- The UK Financial Conduct Authority (FCA) is the AML/CFT supervisor of crypto businesses (cryptocurrency exchange providers and custodians) under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. This means that since January 2020, firms have been required to register for a crypto license and thereafter are subject to FCA supervision and to comply with the same AML/CFT requirements as financial institutions.
- UK law enforcement agencies have the authority to seize crypto assets suspected of being involved in money laundering activities prior to making arrests. This approach helps prevent the movement and dissipation of illicit funds.
- The UK has established specialized units within The National Economic Crime Centre (NECC) and Metropolitan Police Service (MPS) that focus on investigating and prosecuting money laundering and financial crimes. These units leverage technology and blockchain analytics to track and trace illicit financial flows.

- Collaboration between public and private sectors is a cornerstone of the UK's AML/CFT strategy. Initiatives like the Joint Money Laundering Intelligence Taskforce (JMLIT) facilitate information sharing and cooperation between the private sector and law enforcement agencies. While JMLIT has driven successes across multiple investigations the Joint Money Laundering Steering Group (JMLSG), another public-private sector partnership, has proven fundamental to producing formally recognised guidance to assist firms, including VASPs, in understanding and complying with their AML/CFT obligations.

The United Arab Emirates

The United Arab Emirates introduced AML/CFT obligations for Virtual Asset Service Providers (VASPs) through amendments to its principal AML/CFT legislation, Federal Decree-Law No. (20) of 2018. Following these amendments, various regulatory authorities, including the Financial Services Regulatory Authority (FSRA) in ADGM, the Virtual Assets Regulatory Authority (VARA) in Dubai, and the Dubai Financial Services Authority (DFSA) in DIFC, have provided for AML/CFT requirements for VASPs within their respective jurisdictions.

- In 2023, the Central Bank of the UAE (CBUAE) issued guidance for licensed financial institutions to manage AML/CFT risks related to virtual assets and VASPs. In 2024, the CBUAE released the Payment Token Services Regulations, which impose AML/CFT obligations on payment token service providers, ensuring they adhere to stringent standards.
- In line with the risk-based approach, the VASPs are required to conduct risk assessments from an ML/FT perspective. This involves identifying the specific risks the VASP is exposed to and implementing appropriate controls to mitigate these risks.
- VASPs are also required to monitor transactions and report suspicious activities to the Financial Intelligence Unit (FIU) using the goAML platform.

The United States

While the broader cryptocurrency-specific regulatory landscape in the United States is still evolving, it has been clear for over a decade that cryptocurrency businesses are subject to AML requirements and must monitor their platforms for illicit activity. In 2013, the Financial Crimes Enforcement Network (FinCEN) explained that cryptocurrency exchanges constitute money service businesses (MSBs) subject to regulation under the Bank Secrecy Act. In 2019, FinCEN provided additional guidance clarifying which other cryptocurrency businesses met the definition of an MSB and addressing other unique compliance issues related to cryptocurrencies.

- The Bank Secrecy Act (BSA) is the primary legal framework governing AML regulations in the U.S. BSA requires that financial institutions, including cryptocurrency businesses, assist governments with identifying and stopping money laundering activities.
- FinCEN is responsible for creating and enforcing AML regulations, providing guidance for compliance and collecting financial transaction data through reports such as currency transaction reports (CTRs) and suspicious activity reports (SARs).
- The BSA requires financial institutions, including MSBs, to implement a risk-based AML program and to collect and verify their customer's identity, known as Know Your Customer (KYC).

Strategies for crypto-native and non-crypto native scenarios

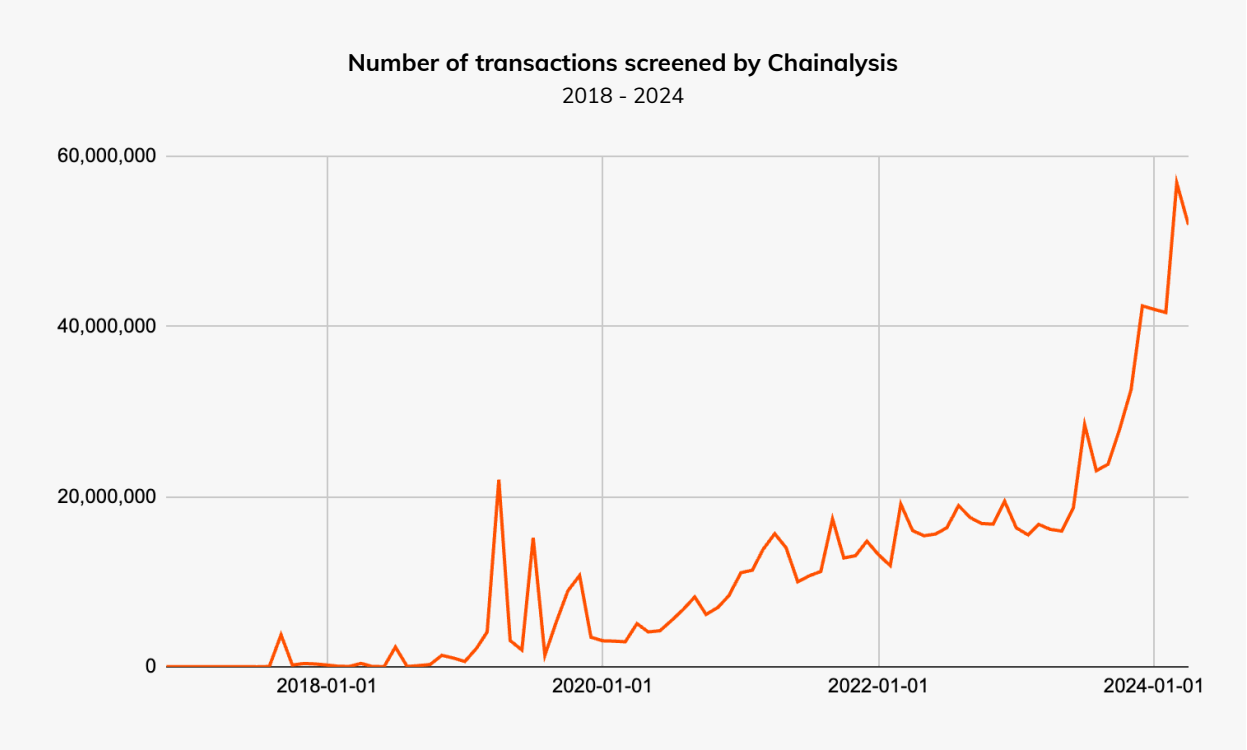
Money laundering touches every aspect of illicit activity, requiring a holistic and adaptive approach to anti-money laundering (AML) and risk management. As blockchain technology evolves, AML strategies must also evolve to counter new tactics and ensure regulations keep pace with technological developments.

Enhanced KYC and AML protocols

Ensuring stringent Know YourCustomer (KYC) and anti-money laundering (AML) measures for both crypto exchanges and traditional financial institutions is imperative. This includes verifying identities, monitoring transactions, and flagging suspicious activities.

Transaction monitoring systems

Both traditional financial institutions and crypto exchanges are increasingly implementing advanced transaction monitoring systems that use machine learning and artificial intelligence to detect unusual patterns indicative of money laundering. Chainalysis Crypto Compliance solutions are increasingly employed by crypto businesses and financial institutions to flag suspicious activity in real-time.



The number of transactions screened by compliance products such as Chainalysis is on the rise, indicating a growing commitment among companies to prevent illicit funds from exiting the ecosystem.

Cross-border collaboration and public-private partnerships

Global cooperation is critical in the fight against money laundering. Criminals often exploit regulatory gaps between jurisdictions, making coordinated international efforts absolutely essential. This includes

harmonizing regulations, sharing intelligence, and conducting joint operations. Collaboration between the public and private sectors to share information and best practices for combating money laundering should be encouraged.

Failing to implement robust compliance programs can have irreparable consequences, including regulatory penalties, loss of consumer trust, and complete exclusion from the financial system. Both traditional and crypto-native financial institutions must prioritize strong AML measures to avoid these risks and ensure the integrity of their operations.

The role of technology and innovation in money laundering prevention

The future of crypto investigations and compliance is fundamentally driven by blockchain intelligence and the power of underlying data to identify suspicious activity for lead generation. Data analysis plays a crucial role in identifying and neutralizing the most pressing threats in the crypto ecosystem — a realm where a single wallet address can illuminate vast networks of criminal abuse.

Balancing privacy and security is essential to protect legitimate users while preventing misuse. Managing compliance costs is also critical to avoid disproportionately impacting small businesses and startups, fostering innovation while maintaining regulatory integrity. As the ecosystem evolves, ongoing education and skill development are also imperative to stay ahead of emerging threats. A deep understanding of blockchain technology and its intersections with criminal activity enables institutions to implement precise controls tailored to their specific risk profiles.

Technology empowers institutions to improve efficiency and outcomes while reducing reliance on cumbersome reporting requirements. Automated systems can quickly analyze large volumes of data, identify risks, and generate actionable insights, improving overall AML effectiveness.

The interplay between blockchain intelligence and data-driven insights is the cornerstone of crypto investigation and compliance. By leveraging advanced technology, managing compliance, and investing in education, the crypto ecosystem can achieve a sustainable and secure framework that fosters innovation while protecting against illicit activities.

Chainalysis

Building trust in blockchains

About Chainalysis

Chainalysis, the leader in blockchain intelligence, makes it easy to connect the movement of digital assets to real-world services. Organizations can track illicit activity, manage risk exposure, and develop innovative market solutions with intelligent customer insights. Our mission is to build trust in blockchains, blending safety and security with an unwavering commitment to growth and innovation. For more information, visit www.chainalysis.com.

FOR MORE INSIGHTS
chainalysis.com/blog

FOLLOW US ON X
@chainalysis

GET IN TOUCH
info@chainalysis.com

FOLLOW US ON LINKEDIN
linkedin.com/company/chainalysis