# Role of Crypto in Money Laundering

## Abstract

This paper examines the role of crypto-assets in money laundering in 2026, focusing on how value actually moves across exchanges, brokers, stablecoin issuers, smart contracts, bridges, and self-custodied wallets. Rather than treating crypto as inherently anonymous or inherently transparent, the paper centers on a practical distinction: public ledgers can make transactions visible while leaving the controlling person unattributed. In this setting, laundering is less about making flows disappear and more about breaking the link between an observable trail and an identifiable actor.

Building on the classic placement, layering, and integration scaffold, the paper reframes crypto laundering as a set of functions that can occur in different orders or in parallel: ingest value, break linkages, move across rails and jurisdictions, store value, and exit or spend. It then develops a threat model mapping key ecosystem actors and control points, and catalogs operational typologies used in contemporary cases, including chain hopping, peel chains, micro-splitting, mixers and coordinated privacy schemes, DeFi routing, cross-chain bridging, stablecoin-centric transport, and laundering-as-a-service markets.

The paper also assesses detection and policy responses, emphasizing risk-based compliance duties for regulated service providers, Travel Rule implementation frictions, sanctions and enforcement leverage, and the limits posed by self-hosted wallets and non-custodial protocols. Finally, it proposes an evaluation framework with measurable metrics for coverage, detection, disruption, reporting quality, and displacement, aiming to move the debate from slogans toward outcomes.

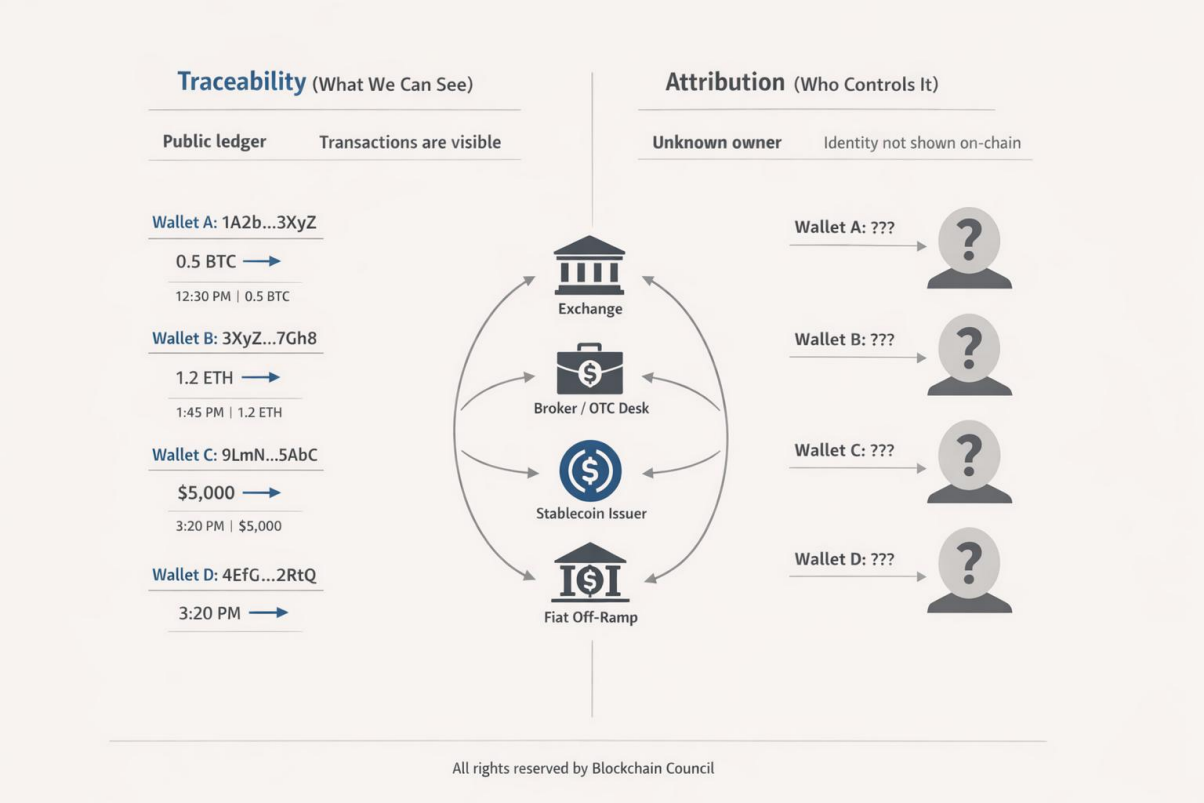
**Keywords**

Crypto-assets; money laundering; virtual assets; VASP; CASP; stablecoins; Travel Rule; blockchain analytics; DeFi; cross-chain bridges; mixers; sanctions evasion.

## Introduction

Crypto-assets are now routine infrastructure for moving value across borders. That reality carries legitimate uses, but it also supports money laundering at scale. By 2026, the relevant question is no longer whether crypto can be abused. It can. The operational questions are harder and more useful: which assets and rails are most frequently exploited; which actors still create choke points that can identify, block, or freeze; how offenders adapt when those points tighten; and which legal duties meaningfully fit systems built from both regulated intermediaries and autonomous software.

A common public misconception is that crypto laundering is primarily about anonymity. Most major blockchains publish transaction histories that can be traced for years. The core friction is not visibility but attribution. An address can be observed without revealing who controls it. This creates a persistent contest between traceability and identification, and it shapes both laundering tactics and the feasible responses. Criminals seek to keep addresses unattributed or to contaminate attribution with false identities, nominees, mule networks, and jurisdiction shopping. Defenders seek to reconnect on-chain movement to off-chain identity through regulated touchpoints, investigative powers, intelligence, and forensic work.



Money laundering is often described through the three-stage model of placement, layering, and integration. That model remains analytically useful, but crypto changes how these stages appear. In many cases proceeds begin in crypto, such as ransomware payments, online fraud receipts, theft from hacks, or scam transfers. When the proceeds originate in crypto, the "placement" stage may be compressed or look invisible, because value is already inside the transfer system at the first moment of receipt. In other cases, placement occurs through fiat-to-crypto gateways, including exchanges, brokers, OTC intermediaries, kiosks, and peer-to-peer markets. Layering is often accelerated by automation and composability, including rapid asset switching, cross-chain routing, and interaction with smart contracts that generate dense transaction graphs. Integration frequently concentrates around cash-out and spending moments that reconnect crypto flows to real-economy use, and those moments often drive both compliance attention and law enforcement leverage.

This paper addresses these realities through a practical threat-model lens. It treats crypto laundering as workflows built from modular building blocks. The building blocks are observable: how value is ingested into crypto form; how wallets split, recombine, and time transactions; which assets are used as routing or storage instruments; where services and protocols are touched; how bridges and wrapped representations shift value across networks; and where and how value

exits into fiat or goods. The goal is not to moralize about the technology, but to clarify how laundering functions emerge from system design, market structure, and uneven regulation.

The paper asks four main research questions.

First, how should laundering be defined and operationalized in crypto contexts where proceeds may originate on-chain and where transaction histories are publicly visible but identity is not?

Second, which typologies are most operationally relevant in 2026, and what indicators can be measured to detect and triage them in real compliance and investigative settings?

Third, where do effective control points exist, and how do those points differ across centralized services, stablecoin issuers with freeze authority, and decentralized arrangements with limited or contested accountability?

Fourth, how can regulators, institutions, and researchers evaluate whether controls are working, beyond counting rules adopted or tools deployed?

To answer these questions, the paper proceeds in three parts. Chapter 1 establishes foundational concepts, definitions, and the crypto laundering threat model. It sets out a functional framing that complements placement, layering, and integration by focusing on the

laundering functions that offenders must accomplish: ingest value, break linkages, move across rails and jurisdictions, store value, and exit or spend. It clarifies what "crypto" means in 2026 by distinguishing coins, tokens, stablecoins, NFTs, wrapped assets, and cross-chain representations, since each category creates different laundering paths and different enforcement leverage. It maps ecosystem actors and the infrastructure that shapes laundering opportunity, including hosted and self-hosted wallets, exchanges and brokers, OTC desks, miners and validators, stablecoin issuers, DeFi protocol operators and interfaces, and analytics providers. Throughout, it emphasizes the central analytic tension between traceability and attribution.

Chapter 2 develops a typology-based view of laundering pathways. It describes placement routes that include cash-to-crypto and bank-to-crypto conversion through exchanges and brokers, peer-to-peer markets, kiosks, and mule networks, as well as crypto-native proceeds. It then details on-chain layering mechanics such as chain hopping, peel chains, micro-splitting, timing strategies, and the use of routers and aggregators that increase hop density. It covers obfuscation services and privacy-enhancing schemes, including mixers and coordinated transaction patterns, and it explains the investigative constraints introduced by privacy-focused assets and shielded transfers. It also analyzes DeFi-based layering patterns,

cross-chain laundering through bridges and wrapped assets, and stablecoins as preferred transport rails due to speed, liquidity, and reduced volatility. The chapter concludes with measurable indicators and red flags that combine behavior and counterparty exposure, along with a reproducible case-mapping workflow designed to support comparable analysis.

Chapter 3 evaluates detection, regulation, and enforcement responses through 2026. It explains compliance duties in practice for regulated service providers, including customer due diligence, ongoing monitoring using on-chain exposure analysis, suspicious reporting, and recordkeeping. It examines Travel Rule implementation as an operational and interoperability problem as much as a legal requirement, and it discusses the frictions created by transfers involving self-hosted wallets. It then compares regulatory models and enforcement levers, including licensing and supervision approaches, sanctions and interdiction strategies, and the practical reliance on compelled records and cooperation from intermediaries. It addresses the hard problems of accountability in non-custodial protocol settings and the policy tensions between privacy rights and crime control. Finally, it proposes an evaluation framework that emphasizes measurable outcomes: coverage of regulated touchpoints, detection precision and speed, disruption and recovery rates, reporting quality, and displacement of illicit flows to alternative rails and jurisdictions.

Two scope decisions are important. First, the paper treats "crypto-asset" and "virtual asset" as near-synonyms but uses the terminology that matches the framework under discussion, since definitions vary across jurisdictions and institutions. Second, the paper focuses on money laundering and closely related illicit finance objectives such as sanctions evasion, while recognizing that similar transaction patterns can reflect different underlying offenses and motivations. As a result, typology indicators are treated as risk signals that require context and, where possible, off-chain corroboration.

The intended contribution is practical clarity. Crypto laundering is often discussed in absolutes, either as untraceable or as trivially traceable. Neither view matches operational reality. The paper's threat model and typologies aim to support analysis that is specific enough to be tested, monitored, and improved. Its evaluation framework aims to support accountability by asking whether controls reduce illicit throughput, increase friction, and improve recovery, rather than whether controls merely exist.

## Chapter 1: Foundations, Concepts, and the Crypto Laundering Threat Model

This chapter sets the base for analyzing how crypto-assets are used to launder money. The goal is not to praise or condemn the tools. It is to describe how value moves, where control points exist (or fail), and

what “laundering” looks like when the financial system is a mix of exchanges, smart contracts, stablecoin issuers, bridges, and self-custodied wallets. By 2026 the question is not whether crypto can be used for laundering. It can. The harder questions are practical: which assets and rails are abused most often, which actors still create choke points, how criminals change tactics when those points tighten, and which legal definitions and duties actually fit how these systems work.

A second theme runs through the entire chapter: public ledgers make many transactions visible, but they do not automatically identify the person behind an address. That creates a constant tug-of-war between traceability and attribution. The ledger can be open. The owner can still be unknown. Crypto laundering, in turn, is less about “hiding” and more about breaking the link between a trail that can be seen and a person who can be named.

## 1.1 Money laundering basics: placement, layering, integration in a digital context

Money laundering is commonly described in three stages: placement, layering, and integration. Placement brings criminal proceeds into the financial system. Layering disguises origin and control through transactions and intermediaries. Integration returns value to the

criminal economy in a form that looks legitimate. This framing appears in UNODC materials and many national AML systems.

Crypto-assets do not remove these stages, but they change how they show up in practice. Timing changes. Signals change. In some cases "placement" is hard to see or feels almost missing. UNODC's cybercrime materials note that when proceeds begin in crypto, the value may already be "in system" at the moment it is received. That compresses the early phase: the criminal does not need to "place" cash into a bank if the payment or theft happened in crypto.

For crypto-enabled cases, a better lens is to treat laundering as a set of functions that can happen in different orders, repeat, or run in parallel:

1. **Ingest value** (convert or receive it into a usable form).

2. **Break linkages** (reduce how easily investigators can connect the funds to the predicate offense).

3. **Move across services and borders** (shift rails, jurisdictions, and counterparties).

4. **Store value** (reduce seizure risk and manage volatility or liquidity needs).

5. **Exit or spend** (cash out or use the value while keeping attribution risk acceptable).

Seen this way, "placement-layering-integration" still matters as a scaffold, but it is not a strict pipeline. In crypto cases, criminals often do placement and early layering at the same time, or they begin with crypto and jump straight to layering tactics.

**Placement in a digital context** often falls into four routes.

**(1) Fiat-to-crypto ingestion.** Here, illicit cash or bank funds are converted into crypto-assets using gateways such as centralized exchanges, brokers, crypto ATMs, payment processors, peer-to-peer (P2P) marketplaces, or OTC intermediaries. This route looks most like classic placement because it touches entities that can run standard AML controls: customer checks, transaction monitoring, suspicious

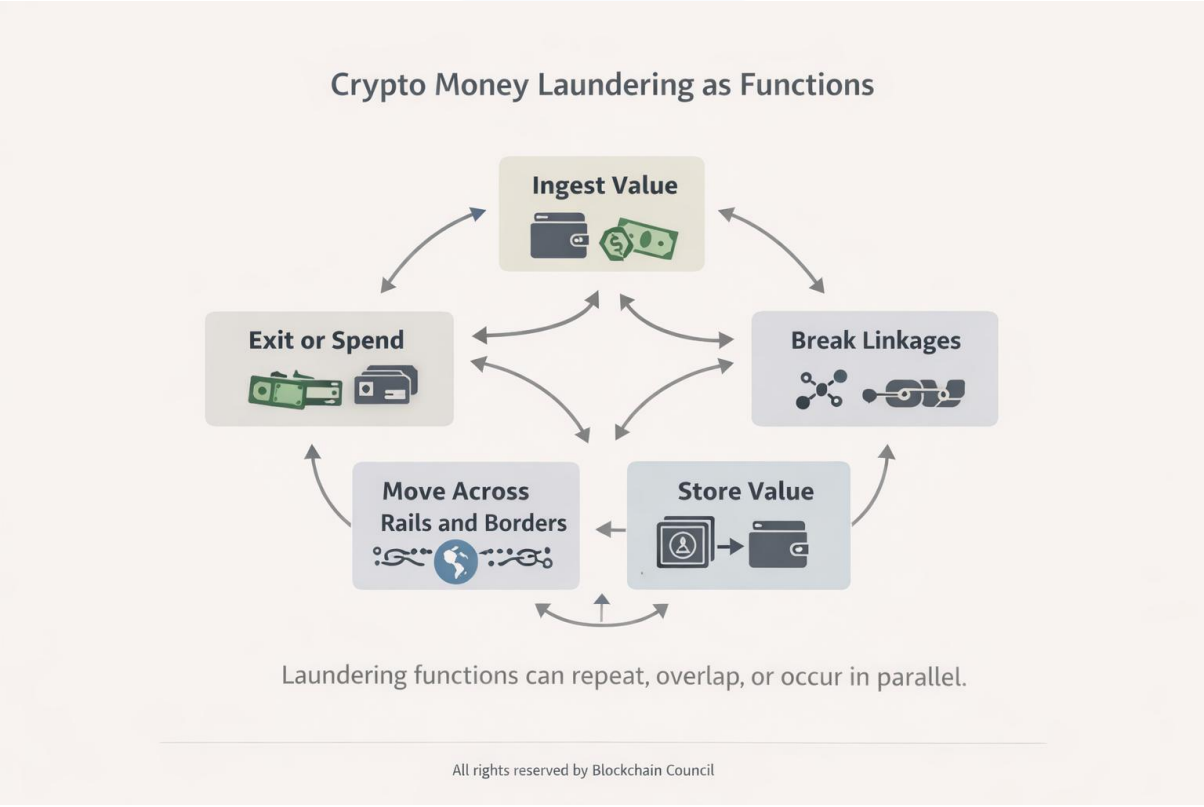
reporting, sanctions screening, and cash limits. FinCEN's attention to kiosks reflects a practical point: retail fraud and scam proceeds often enter crypto through cash-accepting machines and kiosk networks.

**(2) Crypto-native proceeds.** Many predicate crimes now generate proceeds directly in crypto: ransomware payments, online fraud, darknet market sales, theft from hacks, and investment scams. In these cases the offender starts with a wallet they control. Laundering begins immediately, because the first problem is not "getting money into the system," but making sure the wallet does not become an easy seizure target. The early steps are aimed at dispersal, control, and distance from the original event.

**(3) Value tokenization.** Criminal proceeds can be converted into other crypto-asset forms, including stablecoins or tokenized claims, to reduce volatility, improve liquidity, or use rails that move quickly across borders. Stablecoins matter here because they keep a relatively stable unit of account while keeping much of crypto's portability. That changes incentives (less fear of price swings) and changes signals (movement looks like payment flow rather than speculative trading). FATF has flagged growing stablecoin use by illicit actors as a risk that countries should watch and address.

**(4) Institutional camouflage.** Some placement is carried out through front companies, professional facilitators, and layered corporate

structures that buy crypto through multiple accounts, multiple venues, or offshore entities. The goal is to create a believable source-of-funds story and obscure the people in control. Europol communications around large fraud cases often describe networks using many exchange accounts and cross-border corporate setups. In functional terms, this is placement plus early layering, designed and executed together.




**Layering in crypto** relies on many of the same ideas as traditional layering (more steps, more intermediaries, more confusion). But crypto adds built-in tools that can increase ambiguity or cost investigators time. Common mechanics include:

- **Splitting and later recombining.** Funds are divided across many addresses (including “peel chains” and micro-transfers) and then regrouped later. This makes it harder to treat a single transaction path as the whole story.

- **Service hopping.** Criminals move value across exchanges, brokers, OTC desks, and payment processors to fragment visibility and take advantage of uneven controls.

- **Asset hopping.** Funds are converted between assets (for example BTC to ETH to stablecoin to a privacy-focused asset), sometimes using wrapped versions, to complicate tracing and to exploit different market structures and compliance gaps.

- **Cross-chain movement.** Bridges and swap routes that cross several networks raise investigative cost and expand the number of services and jurisdictions that must cooperate.

- **Mixing and privacy tooling.** Mixers, tumbler services, CoinJoin-style coordination, privacy wallets, and privacy-focused networks aim to break on-chain linkability.

- **DeFi layering.** Funds are routed through decentralized exchanges, lending and borrowing protocols, derivatives venues, liquidity pools, and automated strategies. These steps can generate dense transaction graphs that are expensive to interpret and can be arranged to create confusion.

**Integration** is the point where laundered value is used: spent, invested, or converted into goods and services in the real economy. In crypto-enabled laundering, integration often takes one of these forms:

- **Cash-out.** Conversion to fiat through exchanges, OTC brokers, payment processors, money mules, or cash-heavy businesses. This moment is often the most visible to compliance systems because regulated entities must connect movement to an account holder and assess source of funds.

- **Direct spending.** Use of crypto to pay for goods and services (high-value items, gift cards, online services, travel, or cross-border payments). Criminals may prefer spending routes with minimal identity checks or with intermediaries who absorb scrutiny.

- **Investment and asset acquisition.** Purchase of real estate, luxury goods, securities-like exposures, or business interests using fiat obtained from cash-out or via crypto-backed financing. In these scenarios, integration often shows up as "clean-looking" fiat that is presented as business revenue, consulting income, or profits from trading.

One analytic point matters throughout: crypto laundering is not automatically anonymous. Many major chains publish transaction histories. What changes is the link between visibility and identity. The ledger may show the path. It may not show who walked it. Laundering becomes a contest between the criminal's ability to keep addresses unattributed and the defender's ability to reconnect them to

people through regulated choke points, intelligence, and forensic work.

### 1.2 Why crypto is attractive for laundering: speed, access, fragmentation, mechanization

Crypto's appeal to launderers is operational rather than mysterious. These tools can reduce friction, widen options, and turn "money movement" into repeatable workflows that scale beyond local networks.

**Speed and settlement.** Crypto transfers can settle quickly, often within minutes, across borders, outside business hours, without correspondent banking. Speed reduces the time defenders have to react. When a victim sends a bank transfer, institutions may sometimes recall or freeze. When a victim buys stablecoins and sends them to a scam address, the funds can be swapped, bridged, and dispersed before traditional response steps even begin. FATF discussions of cyber-enabled fraud ecosystems describe how this compression supports coordinated laundering that runs across jurisdictions.

**Global reach and liquidity.** Major crypto markets, especially for large assets and stablecoins, provide deep cross-border liquidity. Criminals can find counterparties in many regions, including places with weak supervision or uneven enforcement. FATF's repeated

implementation updates stress that uneven global rules create gaps that offenders can route around.

**Fragmentation and jurisdiction shopping.** Crypto laundering benefits from fragmentation: many networks, many assets, many service providers, and many legal regimes with different definitions of who is regulated. A launderer can spread activity across chains, venues, and wallet clusters so that no single entity sees the full pattern. This is not just an accident of the market; it is a usable feature for criminals.

**Bots, scripts, and "money movement as code."** Smart contracts and trading bots allow repeatable laundering steps: repeated swaps, timed dispersal, liquidity pool interactions, and bridge routes, executed at low marginal cost. A single operator can coordinate many wallets and routes in parallel. The same toolchain that supports legitimate trading also supports repeatable laundering workflows.

**Stable value transport.** Early crypto laundering carried volatility risk. Stablecoins reduce that problem. They allow storage and transfer in units close to fiat while preserving portability and speed. Central banks and supervisors increasingly flag stablecoins as a risk channel because they can function like portable "electronic cash" holdings with low friction.

**Pseudonymity with selective identity exposure.** Crypto systems often allow users to keep identity off-chain and reveal it only when needed (typically at on-ramps and off-ramps). This supports strategies that reduce contact with regulated entities. When contact is necessary, criminals can use nominees, layered companies, forged documents, or regulatory arbitrage between jurisdictions.

**Adaptation under pressure.** When a service is disrupted or sanctioned, criminals move. The past few years have shown cycles of mixer takedowns or sanctions actions followed by shifts to substitutes, new techniques, or heavier use of cross-chain routes and DeFi tools. US action against major mixers illustrates both the pressure and the ecosystem's ability to change tactics.

**Scale indicators.** Public reporting in early 2026 cited estimates that crypto money laundering reached at least $82 billion in 2025, linked in part to fast-growing laundering networks offering escrow-like "guarantee" services and large wallet clusters. A BIS publication estimated crypto used in illicit activities at $51.3 billion in 2024 and noted such figures are likely lower bounds. Methods differ and numbers should not be treated as precise, but the direction is hard to ignore: laundering is not a minor side channel. It is a steady mode of abuse that grows alongside adoption, scams, and cybercrime.

### 1.3 What "cryptocurrency" means in 2026: coins, tokens, stablecoins, NFTs, wrapped assets

"Cryptocurrency" is a loose term. For research, it needs tighter use because different crypto-assets create different laundering paths.

A practical technical definition is: **a crypto-asset is a digital unit of value or rights that can be stored and transferred electronically using distributed ledger technology or similar systems.** Legal definitions vary, but the EU's MiCA framework offers a clear reference because it sets categories and market roles across a large jurisdiction. MiCA covers many crypto-assets not already governed by existing EU financial services law and creates rules for issuance and service provision, with specific treatment for asset-referenced tokens and e-money tokens (stablecoin-like categories).

**Coins.** Coins are native assets of a blockchain (BTC on Bitcoin, ETH on Ethereum). They pay transaction fees and support the network's operation and security. They tend to be liquid and widely supported, so they are often used as intermediate "routing" assets in laundering paths.

**Tokens.** Tokens are issued on top of a chain through smart contracts (for example ERC-20 tokens on Ethereum). They can represent utility, governance, claims on reserves, synthetic exposures, or speculative instruments. Tokens increase laundering options by expanding

conversion paths and creating niche markets and venues where controls may be weaker.

**Stablecoins.** Stablecoins are tokens designed to maintain stable value, often pegged to fiat. Under MiCA's taxonomy, stablecoin-like instruments include e-money tokens and asset-referenced tokens, with specific requirements for issuers and service providers. Stablecoins matter for laundering because they reduce volatility and are widely accepted across exchanges, OTC markets, and DeFi. FATF has warned that stablecoins are being used more often by illicit actors and need risk controls.

**NFTs.** NFTs are unique token identifiers linked to digital items or claims. Their laundering relevance is not that the media file is special. It is that NFTs can act as high-variance vehicles for value transfer, self-dealing, and wash trading, sometimes with a plausible story ("art sale") similar to parts of the traditional art market. Chainalysis has reported wash trading patterns and some illicit flows into NFT marketplaces while noting that measured illicit volumes in early NFT markets were small relative to broader crypto laundering. The structural risk is familiar: thin markets, subjective pricing, and easy self-transacting.

**Wrapped assets.** Wrapped assets are token representations of an asset from another chain (for example, wrapped BTC on Ethereum). They

exist because liquidity and applications are spread across networks. For laundering, wrapped assets allow cross-ecosystem movement without touching fiat, while complicating tracing across wrapping mechanisms and bridge contracts.

**Bridged assets and cross-chain representations.** Bridges move assets between chains. The destination chain often receives a representation minted after locking or burning on the source chain. This can disrupt tracing continuity, especially where bridges use pooled liquidity, intermediate addresses, limited logging, or complicated routing. It can also create multiple "versions" of an asset that can be swapped and recombined.

**Derivative and staking-related tokens.** By 2026 many chains support staking and liquid staking derivatives (tokens representing staked positions). These instruments add more asset types that can carry value and generate cashflow-like patterns. Launderers may point to yield narratives to explain balance growth, but the day-to-day advantage is usually simpler: more venues, more steps, and transaction graphs that take longer to interpret.

The research implication is plain: "crypto" is not one risk. Risk depends on asset type, liquidity, who sits in the compliance perimeter, and what a user can do without identity checks. A stablecoin transfer between two hosted wallets at regulated institutions has a different

risk profile than a bridge-mediated move from a self-hosted wallet into a DEX and then into a privacy-focused asset.

### 1.4 Key ecosystem actors: users, brokers, exchanges, custodians, OTC desks, miners and validators

Crypto-enabled laundering is not just "the blockchain." It is a system of people and organizations with different incentives and powers. A usable threat model asks: who can do what, who can block or freeze, and where duties can attach in practice.

**Users (retail and institutional).** Legitimate users include retail holders, traders, and businesses using crypto for payments or treasury. Illicit users include criminals who generate crypto proceeds (hackers, scammers, darknet vendors) and specialist launderers who sell services to others. In many large cases, the person laundering is not the person who committed the predicate offense. They are a separate operator with skills, infrastructure, and contacts.

**Brokers and payment intermediaries.** Brokers help convert between fiat and crypto, sometimes outside exchange order books. Payment processors support merchant acceptance and conversion. These businesses are high-value control points because they touch identity, bank accounts, and contractual relationships that can be used to enforce compliance.

**Centralized exchanges (CEXs).** Exchanges concentrate liquidity and therefore appear frequently in laundering paths. They can also run AML programs at scale: identity checks, sanctions screening, travel rule processes, transaction monitoring, and suspicious reporting. The weakness is uneven supervision across jurisdictions and the presence of high-risk exchanges that run weak controls. FATF has repeatedly warned that gaps in regulation and supervision create openings that criminals use.

**Custodians and hosted wallet providers.** Custodians hold assets for clients. Hosted wallet services can operate in similar ways. Custody matters because it comes with control: the ability to freeze or block, and the ability to provide records to investigators. It also creates an accountable entity. Under MiCA many such businesses fall under the category of crypto-asset service providers (CASPs), with authorization and operational requirements.

**OTC desks and brokers.** OTC desks execute large trades off-exchange. Many are legitimate and regulated, serving institutional clients. But the channel can attract launderers who want discretion, fewer visible order-book footprints, and negotiated settlement. Risk rises when OTC activity sits inside informal networks, lightly supervised firms, or cross-border arrangements.

**Miners and validators.** These actors secure networks and process transactions. They typically do not have direct relationships with the transacting users and cannot run customer checks in the normal way. Their AML relevance is indirect: protocol-level resistance to censorship, transaction ordering (including MEV-related dynamics), and the limits of enforcing sanctions or blacklists at the base layer. Some validators or mining pools may apply filtering, but practice varies and remains contested.

**Stablecoin issuers.** Issuers can be central actors because many stablecoin designs allow the issuer to freeze tokens or addresses. That creates a strong intervention point, but it also concentrates control and raises governance questions.

**Developers, DAO governors, and protocol operators.** In DeFi, there may be identifiable teams controlling front ends, admin keys, upgrades, or fee mechanisms. Whether these actors are treated as regulated service providers is a central policy dispute. FATF guidance argues that countries should look for responsible persons or entities who may fall within the VASP concept even when a product is marketed as “decentralized.”

**Blockchain analytics firms.** These firms are not transaction infrastructure, but they are enforcement infrastructure. They produce address clustering, attribution hypotheses, and risk scoring used by

exchanges and law enforcement. Their methods matter because they shape what gets flagged and what is missed.

**Regulators, FIUs, and law enforcement.** These bodies set duties, supervise compliance, and investigate. In the EU, the creation of AMLA is intended to reduce cross-border supervision and harmonization problems, with direct supervision of selected high-risk entities expected to begin in 2028.

A clear theme emerges from this actor map: duties attach most easily where there is (1) a stable legal entity, (2) some control over funds or access, and (3) a customer relationship that allows identity collection. As activity shifts toward self-custody, autonomous smart contracts, and cross-chain routing, AML becomes more dependent on perimeter controls, tracing, and targeted enforcement, rather than routine gatekeeping inside a single institution.

### 1.5 Core infrastructure: wallets (hosted vs self-hosted), smart contracts, bridges, DEXs

Infrastructure shapes what laundering paths are possible and how expensive it is to follow them.

**Wallets: hosted vs self-hosted.** A wallet is a key-management tool that allows control over crypto-assets. Hosted wallets are provided by custodians or exchanges; the provider controls private keys and can

apply policies (freezes, blocks, reporting). Self-hosted (unhosted) wallets are controlled by the user with no intermediary. This split sits at the center of regulatory debate because hosted wallets fit the "obliged entity" model and self-hosted wallets do not. EU transfer rules address information duties for certain crypto-asset transfers, and policy discussions often treat self-hosted wallets as higher-complexity for risk control because there is no accountable intermediary.

**Smart contracts.** Smart contracts are on-chain programs that can hold and move value under coded rules. For laundering, smart contracts enable:

- automated swaps (DEXs), lending, borrowing, and derivatives;
- rapid creation of complex transaction graphs at low marginal cost;
- composable routing across several protocols in one logical sequence;

- the creation of "noise," where activity looks like ordinary trading volume, making illicit flows harder to isolate.

Smart contracts also change enforcement. A completed transaction is typically final. There may be no operator who can reverse it, and control may be distributed through governance rules rather than a single company.

**Decentralized exchanges (DEXs).** DEXs allow asset swaps without a centralized intermediary holding customer accounts. Liquidity is provided through pools or order-book-like mechanisms. For laundering, DEXs support asset hopping and layering without protocol-level identity checks. For defenders, controls often sit at the edges: user interfaces, aggregators, bridges, analytics, and fiat gateways.

**Bridges.** Bridges transfer assets between chains. They may be custodial (a trusted intermediary holds assets) or rely on multi-signature or other verification methods. For laundering, bridges matter because:

- they make chain hopping routine;

- they can disrupt analytic continuity, especially where pooled liquidity, intermediate addresses, or limited logging are used;

- they add operators and services that can become targets for enforcement (bridge operators, relayers, interface providers).

**Mixers and privacy services.** Mixers pool funds and return different outputs to break transaction linkability. Tornado Cash became a reference point because of enforcement action and legal dispute. US Treasury sanctioned Tornado Cash in 2022 and described its use in laundering; later public reporting described sanctions being lifted in 2025 while criminal cases against individuals linked to the service continued. Regardless of how any single service is treated, the functional point stands: mixing competes directly with tracing.

**Layer-2 networks and rollups.** Many ecosystems rely on scaling layers that batch transactions and post summaries to base chains. These systems can reduce what is visible at the base layer and introduce new intermediaries such as sequencers and bridge contracts. For AML analysis this means tools and investigations must follow

activity into L2 environments and account for differences in data access and indexing.

**Oracles and cross-system connectors.** Oracles feed outside data into smart contracts. They are not a direct laundering tool, but oracle-based protocols can create transactions whose purpose is hard to infer from on-chain data alone. That matters for classification and monitoring, because it becomes harder to separate payment flow from internal strategy moves.

The main takeaway is simple: laundering thrives where value can move without identity checks and where interpretation is expensive. Infrastructure that increases optionality, composability, and cross-chain mobility increases laundering surface area unless the surrounding control environment tightens to compensate.

### 1.6 Privacy and traceability: pseudonymity, address clustering, attribution limits

Crypto's most misunderstood property is not anonymity but pseudonymity. Most major chains publish transaction histories. What is missing is an automatic map from address to person. The AML contest is therefore centered on attribution.

**Pseudonymity as default.** Public blockchains expose addresses, amounts, and timing. Anyone can observe flows, but cannot assume

who controls an address. This is different from banks, where institutions have identity records but outsiders do not see internal ledgers.

**Address clustering and heuristics.** Analytics systems try to infer which addresses are controlled by the same actor using heuristics such as multi-input spending patterns, change address behavior, timing patterns, reuse, and behavioral similarity. These methods can be effective, but they are probabilistic and vary by asset and chain design. They also have countermeasures. The research implication is restraint: clusters are hypotheses unless confirmed by off-chain evidence such as KYC records, seizures, communications, or device forensics.

**Attribution through choke points.** Attribution often happens when an address touches a regulated or semi-regulated entity: an exchange deposit, a broker transaction, a stablecoin issuer action, or a payment processor. This is why cash-out attempts show up again and again in investigations. It is also why criminals try to reduce the number of such touchpoints or contaminate them through false identities.

**Adversarial tactics that strain attribution.** Criminals use many tactics to reduce linkability and make clustering less certain:

- one-time addresses and avoidance of reuse;

- peel chains and scatter patterns that push funds across many addresses;

- chain hopping, especially toward chains with thinner tooling or weaker compliance presence;

- multi-hop swaps through DEX aggregators that create dense graphs;

- mixing and privacy tools that break deterministic links;

- privacy-focused assets and shielded transfers that hide sender, receiver, or amounts;

- mule networks and compromised accounts that insert other people into the flow.

Mixers illustrate the enforcement tension in a visible way. US Treasury has sanctioned several mixers, including Blender and Sinbad, describing their use by DPRK-linked actors to obscure stolen funds. FinCEN has also pursued regulatory approaches aimed at certain classes of mixing-related activity, including proposals for special measures. These moves show a broader pattern: when a ledger is open, criminals pay for tools that add opacity, and defenders try to target the services that sell that opacity.

**Public ledgers as an investigative advantage.** A blunt point often gets missed in public debate: criminals use crypto partly because it is fast and portable, not because it is invisible. The open record can also help defenders. Many major cases rely on on-chain traces that persist over time. FATF and other bodies increasingly point to the use of technology and data capability to pursue complex cross-border cases.

**What on-chain data cannot answer by itself.** Even with full ledger data, investigators often cannot answer basic questions: who is behind

a self-hosted wallet; whether a transfer is payment, theft, or internal shuffling; whether a transaction represents a real change in control; what the predicate offense is. Those questions require off-chain evidence: platform records, communications, IP logs, open-source intelligence, undercover work, and cross-border legal cooperation. Crypto AML is therefore hybrid: on-chain tracing guides hypotheses, and off-chain work proves them.

### 1.7 Risk-based AML/CFT framing for virtual assets: standards, terminology, and obligations

The dominant global AML/CFT framework remains the FATF Recommendations, implemented through national law and assessed through mutual evaluations. FATF updated Recommendation 15 to extend AML/CFT duties to virtual assets and virtual asset service providers (VASPs) and has issued detailed guidance on applying a risk-based approach in this sector. FATF also publishes targeted implementation updates and repeatedly reports uneven adoption, noting that gaps create openings that criminals exploit.

**Risk-based approach (RBA) in practice.** The RBA means controls and resources should match risk. In the crypto-asset sector, common risk drivers include:

- **Customer risk:** anonymity features, geography, beneficial ownership complexity, politically exposed persons, and known

typologies.

- **Product and service risk:** privacy tools, mixers, cross-chain bridges, higher-risk stablecoins, and DeFi services without enforceable controls at the protocol level.

- **Transaction risk:** speed, structuring, chain hopping, contact with sanctioned entities, and links to known illicit clusters.

- **Jurisdiction risk:** weak AML regimes, sanctions exposure, and high levels of cybercrime or fraud infrastructure.

- **Channel risk:** remote onboarding, use of intermediaries, and high-frequency API activity.

**Core duties applied to VASPs (and similar categories).** Under FATF standards and many national rules, regulated virtual asset businesses are generally expected to:

- register or obtain a license;
- conduct customer due diligence, including beneficial owner checks where relevant;
- keep records;
- monitor transactions and report suspicious activity;
- apply sanctions controls;

- follow travel rule-style information duties for certain transfers;
- manage third-party and outsourcing risks;
- apply enhanced checks for higher-risk customers and transactions.

Implementation is difficult because the sector includes both centralized actors that can run conventional compliance programs and decentralized arrangements that do not fit the usual entity-based model.

**EU framing in 2026.** The EU illustrates how definitions and duties are being made operational across a large market.

- **MiCA** creates a harmonized framework for crypto-asset markets, including authorization and conduct rules for crypto-asset service providers (CASPs). It applies fully from 30 December 2024, with stablecoin-related provisions applying earlier (30 June 2024).

- The updated **EU Transfer of Funds Regulation** (Regulation (EU) 2023/1113) extends information duties to transfers of certain crypto-assets, reflecting travel rule objectives and applying from late 2024 alongside broader rollout.

- The EU AML package includes an EU-wide AML Regulation (EU) 2024/1624 that applies from 10 July 2027, aiming to replace fragmented national rules with one rulebook, and creates **AMLA**, headquartered in Frankfurt. Public reporting in early February 2026 stated that AMLA is expected to be fully operational in 2028 and to directly supervise selected high-risk institutions from that time, with crypto-assets named among threats in its planning.

This architecture matters because it clarifies the regulated perimeter (CASPs), information duties for transfers, and a timeline for more centralized supervision. It also shows a limit: even a strong EU framework cannot, by itself, shut down global laundering networks

that route value through non-EU services, self-hosted wallets, or weaker jurisdictions.

**US framing in 2026.** The US approach remains anchored in the Bank Secrecy Act (BSA) and FinCEN's application of money services business duties to convertible virtual currency businesses. FinCEN continues to issue focused notices and advisories on channels such as crypto kiosks, reflecting concern about retail fraud and cash-based ingestion. The US Treasury's DeFi illicit finance risk assessment argues that illicit actors use DeFi services and that gaps persist where compliance duties are unclear or absent. US sanctions policy has also been a major lever, including actions against mixers and other infrastructure used to obscure illicit proceeds, even as court challenges and policy changes illustrate legal constraints and shifting interpretations.

**Friction points: travel rule, self-hosted wallets, and DeFi.** The central tension in crypto AML is the mismatch between entity-based duties and protocol-based value movement.

- **Travel rule goals** are straightforward for bank wires (collect and transmit originator and beneficiary data). They become difficult when transfers involve self-hosted wallets or routing through smart contracts rather than clear intermediaries. EU legislation and industry debates reflect this problem directly.

- **DeFi raises a deeper issue:** if a protocol is widely accessible and runs without a central operator, who is the "service provider"? FATF guidance pushes countries to identify persons or entities with control or sufficient influence who may fall within VASP scope, even when a system is described as decentralized.

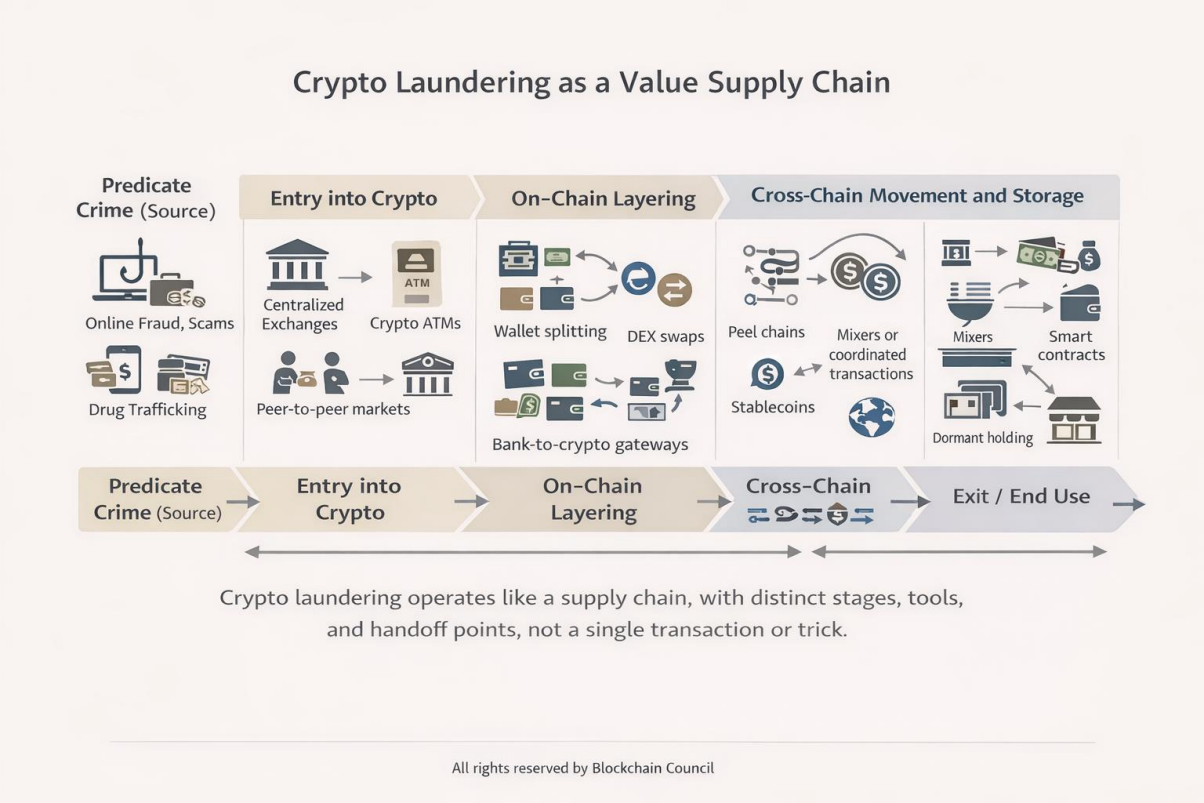
A workable risk-based frame in 2026 therefore requires two strategies at once:
(1) tighten controls where regulated entities exist (CASPs/VASPs, stablecoin issuers, brokers), and
(2) build investigative and enforcement capacity for activity outside routine compliance attachment (self-hosted wallets, autonomous protocols, cross-chain routes), including targeted action against high-impact laundering services.

### 1.8 Working definitions for the paper: illicit finance, laundering typologies, VASP/CASP boundaries

To avoid drift, this paper uses working definitions designed to match both technical reality and common regulatory language.

**Illicit finance (working definition).** Illicit finance refers to the creation, movement, or use of value derived from or meant to support unlawful activity, including money-laundering predicate offenses (fraud, drug trafficking, corruption, cybercrime), terrorist financing, proliferation financing, and sanctions evasion. This scope is wider than "money laundering" because crypto systems are used for several forms of unlawful finance, and similar transaction patterns can serve different goals.

**Money laundering (working definition).** Money laundering is the set of actions used to conceal or disguise the illicit origin, ownership, control, or destination of value, or to make such value appear legitimate, so criminals can use it with lower risk of detection, confiscation, or prosecution. The placement–layering–integration model is treated as a descriptive scaffold rather than a fixed sequence, and crypto-specific variants (including crypto-native proceeds with little visible placement) are included.




**Laundering typologies (working definition).** A laundering typology is a recurring pattern of methods, tools, and actors used to carry out laundering functions. In crypto contexts, typologies are defined by combinations of:

- **Ingestion channel:** exchange, ATM, P2P, OTC, or crypto-native proceeds.

- **Obfuscation method:** splitting, mixing, DEX swapping, chain hopping, bridge routing, privacy-focused assets.

- **Storage strategy:** self-custody, custodial accounts, stablecoins, or DeFi-based holding patterns.

- **Exit channel:** regulated cash-out, OTC, merchant spending, asset purchase, or layering into corporate accounts.

- **Control structure:** single operator, mule network, professional laundering service, escrow or “guarantee” platform.

By 2026, reporting describes professional laundering services and platform-style escrow arrangements as increasingly relevant. Public reporting in January 2026 described large laundering networks using “guarantee” platforms and extensive wallet infrastructure, suggesting a shift toward service-market organization rather than ad hoc laundering.

**Virtual asset (VA) (working definition).** A virtual asset is a digital representation of value that can be traded, transferred, or used for payment or investment, excluding narrow legal representations of fiat, consistent with FATF terminology. This paper treats "crypto-asset" and "virtual asset" as near-synonyms, using "virtual asset" in FATF-aligned discussions and "crypto-asset" in EU MiCA-aligned discussions.

**VASP (working definition).** A virtual asset service provider is any natural or legal person who, as a business, conducts one or more of the following for or on behalf of another person: exchange between virtual assets and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and participation in or provision of financial services related to an issuer's offer or sale of a virtual asset. This follows the FATF framework and anchors the discussion of duties.

**CASP (working definition).** A crypto-asset service provider is the MiCA-aligned EU category for firms that provide regulated crypto-asset services to clients. It broadly overlaps with VASP but is defined within EU law and tied to EU authorization and conduct rules. This paper uses "CASP" for EU-specific duties and "VASP" for global standards or non-EU contexts.

**VASP/CASP boundary rules used in this paper.** The difficult part is not writing a definition. It is deciding how decentralized arrangements fit. This paper applies four boundary rules:

1. **Centralized custody or brokerage usually means a regulated boundary.** If an entity holds customer assets, controls private keys, or intermediates exchange or transfer as a business, it is treated as a VASP/CASP candidate by default.

2. **Interface control can create service-like responsibility.** If a party runs a dominant front end, sets parameters, collects fees, controls upgrades, or retains admin privileges that shape user transactions, the arrangement is treated as having a potentially responsible entity. FATF guidance encourages identifying such entities in DeFi contexts.

3. **Self-directed peer-to-peer transfers sit outside routine service duties, but remain within investigative scope.** Transfers between self-hosted wallets with no intermediating entity are treated as "P2P domain" activity for compliance. That does not mean low risk; it means different controls are needed

(for example, stronger scrutiny at on-ramps and off-ramps, tracing, and targeted law enforcement operations).

4. **Protocol autonomy reduces traditional compliance attachment but does not reduce risk.** Where there is no identifiable operator with control or sufficient influence, duties cannot attach in the usual way. These cases are treated as "non-custodial protocol domain," where risk management depends on perimeter controls, sanctions enforcement on surrounding infrastructure, and investigative capacity.

**Crypto AML threat model (integrated working model).** Combining the above, the threat model used in this paper includes:

- **Adversaries:** (a) retail fraud and scam operators; (b) cybercriminals (ransomware, exchange hacks); (c) organized crime groups laundering trafficking and drug proceeds; (d) professional laundering networks offering laundering-as-a-service; (e) sanctions evaders and state-linked actors; (f) terrorist and proliferation financiers where relevant.

- **Objectives:** move and store value while lowering detection and seizure risk, convert into stable or spendable forms, and reintroduce value into the legitimate economy.

- **Capabilities:** wallet infrastructure, mule networks, access to multiple exchanges and OTC channels, bot- and contract-based transaction routing, cross-chain movement, mixing and privacy tools, and the ability to exploit uneven regulation.

- **Constraints:** eventual need to convert or spend, reliance on liquidity and exchanges, persistent traces on public chains, operational security failures, and targeted enforcement actions.

- **Defender tools:** perimeter compliance (customer checks, monitoring, reporting, travel rule), blockchain analytics and clustering, sanctions enforcement, asset freezing where issuer or custodian control exists, joint investigations and intelligence

sharing, and more harmonized supervision (for example, AMLA's planned cross-border role from 2028).

This model is intentionally practical. It assumes criminals adapt and that compliance is uneven across the world. It also starts from an uncomfortable fact: many of the same tools that support open finance also support large-scale fraud. UNODC reporting on the convergence of casinos, junkets, and crypto-assets in organized crime laundering systems is a reminder that crypto laundering is not a separate universe. It connects to older underground banking and professional facilitation networks.

With these foundations in place, the rest of the paper can move beyond slogans. It can evaluate specific laundering paths, realistic intervention points, and the trade-offs between privacy, openness, and enforceable accountability in the 2026 crypto economy.

## Chapter 2: Laundering Typologies and Operational Pathways Using Crypto

Crypto laundering in 2026 is not one trick. It is a toolkit of repeatable moves that offenders mix and match based on the source of the money (fraud vs hacked funds vs drug revenue), the pressure they face (sanctions, exchange controls, frozen balances), and the outcome they

want (cash-out, long-term storage, spending, or transfer to partners). The best way to study it is as pathways built from observable building blocks: how value is brought in, how wallets behave, how assets are converted, which services are touched, when chains are crossed, and where value exits.

This chapter sets out core typologies and their operating logic, then ties them to indicators and red flags that can be tracked and tested in case studies.

## 2.1 Entry points and "placement" routes: cash-to-crypto, P2P markets, ATMs, money mules

In crypto cases, "placement" often means converting cash or banked proceeds into crypto-assets, or taking proceeds already in crypto and shifting them into assets that are easier to move or hold (often stablecoins). The problem for the launderer is basic: get value into crypto without getting blocked, named, or stuck. The answer is rarely one channel. It is a mix chosen for speed, low scrutiny, and local availability.

### Cash-to-crypto through centralized gateways

Centralized exchanges and brokers remain high-liquidity on-ramps, but they are also watched closely. Many launderers avoid the largest and most tightly supervised venues at the placement stage unless they

can get around controls using false identities, nominees, layered companies, or compromised accounts. Casework and reporting continue to show that weak compliance at some venues still widens the problem even after major enforcement actions.

Common sub-typologies include:

- **Nominee accounts:** accounts opened with third-party identities, forged documents, or recruited individuals paid to submit KYC materials.
- **Compromised accounts:** takeovers of legitimate exchange accounts (phishing, SIM swaps, stolen credentials) used to place illicit funds and move them out quickly.
- **Layered corporate onboarding:** shell entities and "consulting" stories used to justify large fiat deposits followed by crypto purchases.

**P2P markets and informal exchange networks**

P2P networks can operate with limited formal oversight, often through messaging apps and in-person or local settlement. Even where the platform itself is run by a regulated business, the last-mile settlement may still be bank transfers between individuals, cash deposits, or payment apps—gaps that mule networks exploit.

A recurring pattern in fraud ecosystems is: victim funds enter bank accounts, move through mule accounts, then convert into stablecoins (often USDT) and move offshore. Recent reporting from India describes this pattern plainly: proceeds are routed through multiple accounts and converted into USDT for cross-border movement, while delayed reporting reduces recovery.

**Crypto ATMs and kiosks (CVC kiosks)**

Kiosks offer a cash placement route that can take minutes: cash in, crypto out to a destination wallet. That speed and simplicity are why this channel is strongly linked to scam payments and other illicit activity.

FinCEN's August 2025 notice describes high levels of illicit use involving CVC kiosks and provides indicators for operators and financial institutions. In practical terms, kiosks support:

- **Cash structuring:** repeated purchases kept below reporting or internal thresholds.
- **Victim-directed placement:** scammers instruct victims to use kiosks and send crypto to attacker-controlled wallets, shifting the placement work onto the victim.
- **Mule-mediated placement:** couriers or recruited individuals deposit cash and forward crypto onward.

## Money mules, “mule herders,” and account farming

Mule networks connect bank rails to crypto rails. They supply bank accounts, cards, SIMs, devices, and logins, then use them to receive victim funds, buy crypto, and relay value. Modern mule operations often run like a production line: recruitment, onboarding, credential capture, transaction execution, then escalation into crypto conversion.

Law enforcement reporting from Karnataka describes “mule herders” moving very large volumes through many mule accounts, showing that scale comes from coordination as much as from technical skill. This matters for crypto AML because the conversion step is often where bank visibility ends and crypto movement begins.

## Placement indicators across entry routes

Across these channels, a small set of signals shows up again and again:

- High-frequency small purchases clustered in time (kiosk or P2P structuring).
- Rapid onward transfer to new wallets (minimizing time in view).
- Quick conversion into stablecoins after acquisition (volatility control).

- Repeated transfers to a small set of receiving addresses (service wallets or laundering hubs).

### 2.2 Layering on-chain: chain hopping, peel chains, micro-splitting, timing games

Layering is where crypto's composability becomes useful to criminals. On-chain layering is not about making transactions invisible; it is about making attribution costly, slow, and uncertain. Many ledgers are public. The gap is identity.

#### Chain hopping as a dominant layering strategy

Chain hopping is rapid movement across assets and networks using swaps and bridges to fragment the trail and move into environments with different tooling, different service coverage, or weaker monitoring. Elliptic describes chain hopping as a defining method and notes the use of DEX aggregators and bridges to complicate tracing and avoid actions such as stablecoin freezes.

Operationally, chain hopping does three things:

- **Break continuity:** investigators must follow activity across multiple ledgers, indexers, and attribution systems.
- **Exploit uneven controls:** one chain's ecosystem may have fewer cooperative services or weaker supervision.

- **Work around asset-specific controls:** some stablecoins can be frozen, while some native or privacy-focused assets are harder to freeze.

**Peel chains and gradual dispersion**

A peel chain moves a large balance through a sequence of transactions, “peeling” small amounts off to other addresses or services at each step. This spreads seizure risk and avoids moving everything through one obvious cash-out event. Merkle Science describes this method clearly, and academic work has formalized heuristics for detecting peel chains on Bitcoin.

Peel chains appear in multiple settings:

- laundering after exchange hacks (slow release to reduce alerts),
- darknet vendor cash-outs (regular peels to exchanges or brokers),
- scam proceeds (splitting to several cash-out channels).

**Micro-splitting and UTXO management**

On UTXO-based chains such as Bitcoin, offenders often split funds into many outputs, then spend them in varying combinations to create combinatorial complexity. On account-based chains, micro-splitting

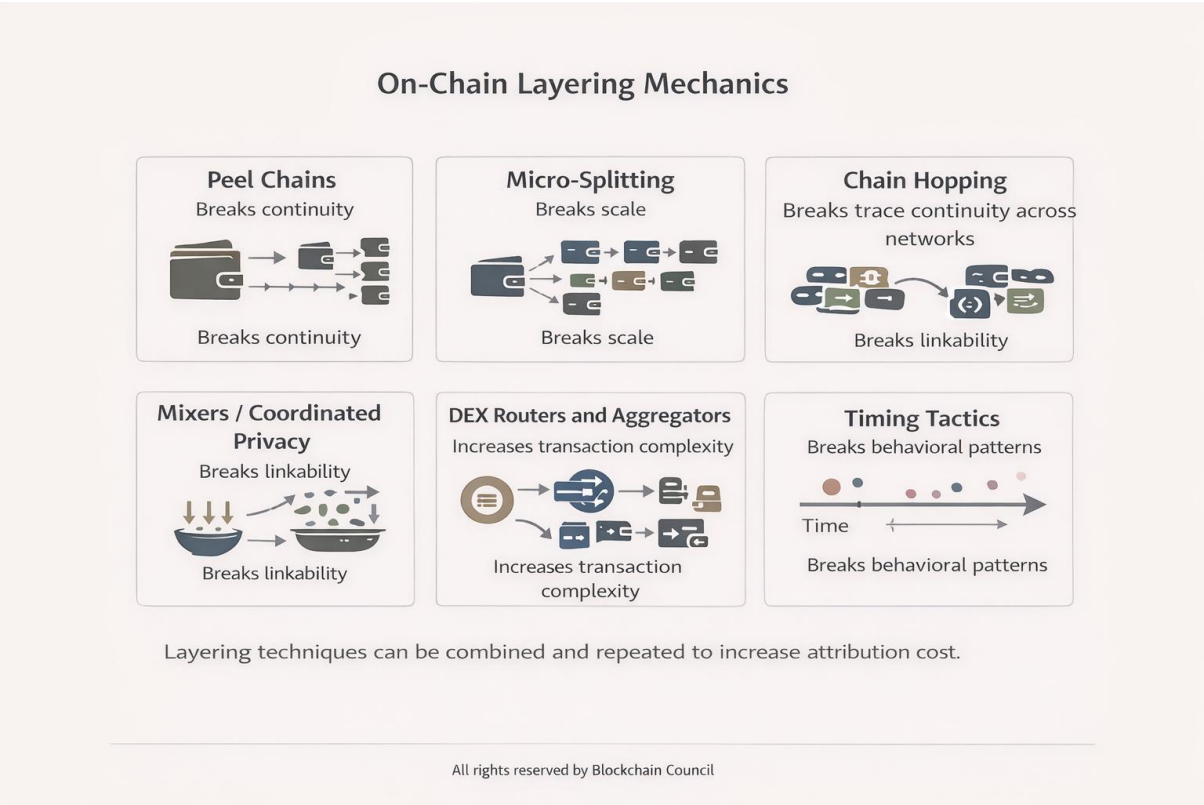
still occurs, but it shows up as many small transfers and swaps across new addresses.

**Timing games and dormancy tactics**

Not all laundering is fast. Time is also used as cover:

- immediate dispersal for fraud proceeds to reduce the chance of intervention,
- dormancy after major hacks, followed by gradual movement months later when attention fades,
- bursts during weekends, holidays, or high-volume market periods to blend into background activity.

As laundering becomes more automated, timing patterns also change. Emerging research discussions describe automated micro-structuring and high-frequency dispersal, sometimes framed as “agentic smurfing,” where scripts run continuous low-level movement that avoids simple thresholds.




## 2.3 Obfuscation services and techniques: mixers, CoinJoin-style coordination, swap routers

Some layering uses ordinary transfers and swaps. Other layering uses tools built to sever links. Three categories matter most: mixers, coordinated transaction schemes (CoinJoin-style), and routing infrastructure (swap routers and aggregators).

### Mixers and laundering services

Mixers pool and redistribute funds to disrupt linkability. They can be custodial (operator takes possession) or non-custodial (smart contracts enforce the logic). Enforcement actions show how central these tools

have been in high-profile laundering, especially in cases tied to large thefts and sanctions evasion.

The US Treasury sanctioned the Sinbad mixer in 2023, alleging it was used to launder proceeds from major thefts including Axie Infinity and Horizon Bridge-related incidents. DOJ has also pursued charges against operators associated with mixing services, reflecting a strategy of targeting facilitators as well as end users.

A major legal complication is that some mixing is implemented through autonomous smart contracts. A US appeals court overturned Treasury sanctions against Tornado Cash in late 2024, finding that immutable smart contracts did not qualify as sanctionable property under the authority used. Public reporting later described sanctions being lifted in 2025 while criminal prosecutions continued against individuals associated with the service. The operational point is unchanged: whether or not one tool is available at a given time, the laundering function persists and offenders route to the next tool that provides it.

**CoinJoin-style coordination on Bitcoin**

CoinJoin is a coordination method in which multiple users combine inputs and outputs into a single transaction, making it harder to map which input funded which output. It can be used for legitimate

privacy, but it has also been used in laundering and has drawn enforcement attention.

The Samourai Wallet case is a key reference point. DOJ and IRS communications describe Samourai as facilitating concealed transfers and laundering, and public reporting covers arrests and charges connected to its mixing services. Technical work explores detection of CoinJoin patterns and the limits of inference.

For monitoring, CoinJoin is a risk marker, not proof on its own. Context matters. CoinJoin plus a link to a known illicit source, plus rapid exchange deposit, plus structuring behavior is far more telling than CoinJoin alone.

**Swap routers, DEX aggregators, and routing as camouflage**

Routers and aggregators route trades across multiple pools and venues to improve execution. They also produce multi-hop swap traces that are hard to interpret quickly, especially when combined with bridges and multi-chain routing. Elliptic notes the use of DEX aggregators in chain hopping sequences, including swapping between stablecoins that can be frozen and other assets.

In laundering terms, routers help by:

- increasing hop density (more contracts and steps per unit value),

- spreading across venues (less dependence on one identifiable pool),
- enabling rapid asset switching to avoid freezes and exploit jurisdiction gaps.

### 2.4 Privacy-focused assets and protocols: risk drivers and investigative limits

Privacy-focused assets and protocols are designed to reduce traceability by hiding transaction details (sender, recipient, amount) or by making linkage inference unreliable. They do not automatically imply criminal conduct, but they change what investigators can do.

**Risk drivers**

- **Reduced on-chain visibility:** when amounts or participants are hidden, tracing can be limited or impossible without other data.
- **Weaker compliance coverage:** some exchanges and custodians restrict or drop support because monitoring is difficult, pushing activity toward higher-risk venues.
- **Direct fit with laundering goals:** privacy features map cleanly onto breaking attribution.

Chainalysis describes privacy coins as crypto-assets with privacy-enhancing features built to reduce traceability. Academic work also

suggests that restrictions can reduce adoption and liquidity, concentrating remaining activity in fewer venues.

**Investigative limits**

Privacy-focused protocols impose practical constraints:

- attribution must lean more on off-chain information (exchange records, device data, human sources),
- seizures can be harder because links to service touchpoints are less direct,
- risk scoring becomes more probabilistic and can generate more false positives if applied bluntly.

From an AML perspective in 2026, the core framing is operational: privacy features increase uncertainty, and uncertainty increases risk. Institutions often respond with stronger due diligence, tighter limits, and stricter counterparty controls when privacy-centric rails are involved.

### 2.5 DeFi laundering patterns: DEXs, lending loops, flash loans, liquidity pools

DeFi laundering is rarely about earning yield. It is about swapping, routing, and reshaping value without protocol-level identity checks,

while generating transaction complexity that overwhelms manual review and can defeat simplistic monitoring.

The US Treasury's DeFi illicit finance risk assessment describes DeFi as layered (settlement, asset, application, interface) and notes that illicit actors can exploit gaps where duties are unclear or absent.

**DEX-centric laundering: swaps as laundering steps**

A common DeFi pattern is straightforward: illicit funds arrive in a self-hosted wallet, then are swapped on a DEX into another asset—often stablecoins for liquidity or native assets to reduce freeze risk. This can repeat across pools and chains.

Indicators include:

- swaps immediately after receiving funds from known-risk sources,
- multiple swaps in short windows with no clear economic reason beyond conversion,
- use of aggregators to increase hop density and blur intent.

**Lending loops and collateral cycling**

Lending protocols can be used to create flows that resemble ordinary finance activity:

- deposit collateral (possibly tainted),

- borrow stablecoins or other assets,
- swap borrowed assets, repay, then repeat.

This can serve two purposes: transform assets through many protocol touchpoints, and create a story of "borrowing" and "trading" that complicates explanations of source of funds.

**Flash loans and synthetic profit stories**

Flash loans allow borrowing without collateral, provided the loan is repaid within the same transaction. They are used for arbitrage and exploits, and they can also be adapted to pack many actions into one atomic transaction. Popular commentary sometimes overstates "flash loan laundering," but the mechanism can still add confusion by generating complex traces inside a single transaction. Treasury's DeFi assessment supports the broader point: composable actions can be abused, especially where there is no responsible intermediary.

**Liquidity pools and wash-volume generation**

Liquidity pools can be used to:

- swap in and out repeatedly to create noise,
- generate fees or volume that looks like trading,
- move through correlated assets (especially stablecoin pairs) with minimal slippage.

For AML monitoring, the task is separating plausible trading from laundering-driven behavior. Useful signals include repeated round trips with consistent losses, extreme hop density with no price rationale, and links to known-risk clusters.

### 2.6 Cross-chain laundering: bridges, wrapped assets, multi-network relay patterns

Cross-chain laundering is now routine. It exists because liquidity and applications are spread across many networks, and because chain transitions can disrupt tracking.

Elliptic notes that laundering often spans multiple blockchains and cites illicit cross-chain flow totals in the tens of billions.

#### Bridge-mediated chain hopping

A common pattern looks like this:

1. receive funds on Chain A (often where the crime occurred),
2. swap into a bridge-friendly asset (often stablecoins or a liquid native asset),
3. bridge to Chain B,
4. swap again (sometimes into a different asset class),
5. repeat, then cash out through a service that offers weaker controls or better liquidity.

Elliptic gives an example of hackers swapping between stablecoins and bridging to Ethereum, then using a DEX aggregator to swap into ETH, plausibly to reduce freeze risk.

**Wrapped assets as mobility tools**

Wrapped assets move value into ecosystems where specific applications and liquidity exist. For laundering, wrapped assets:

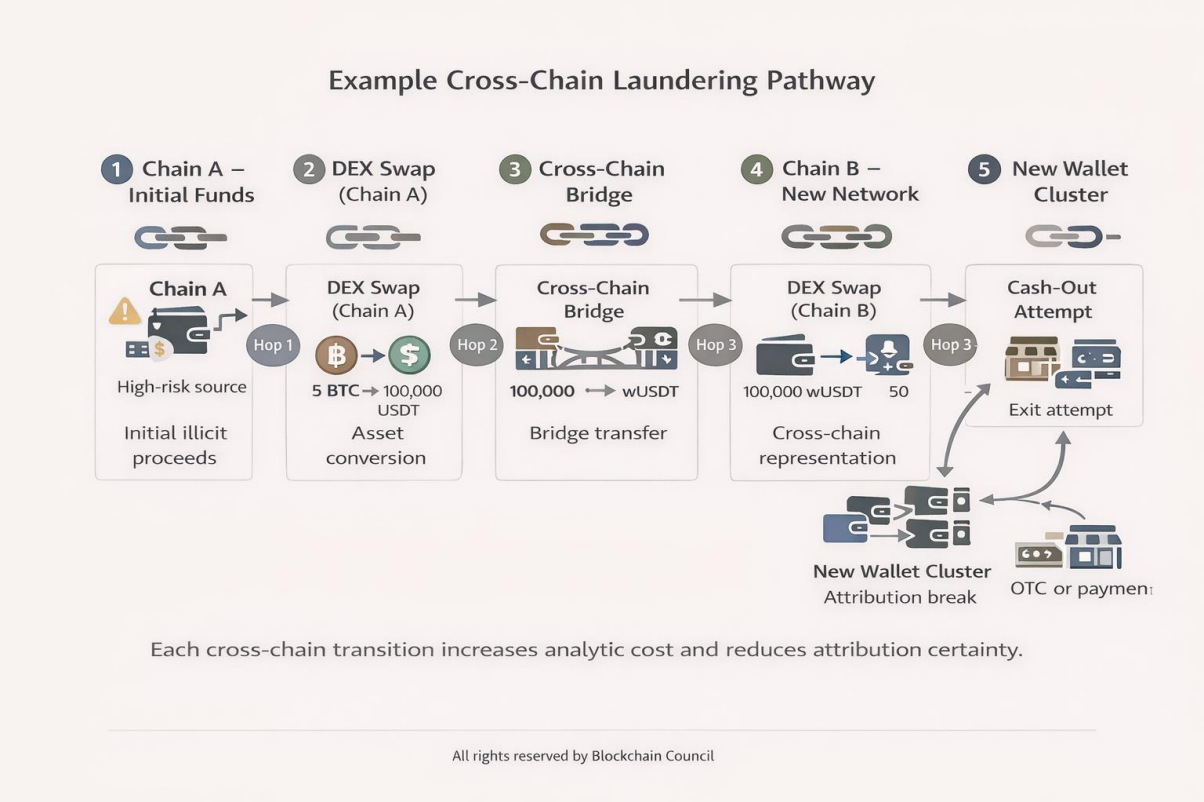
- expand the menu of swap and bridge routes,
- create multiple representations of the same economic value, complicating tracking,
- allow movement without returning to fiat, reducing exposure to regulated gateways.

**Multi-network relay and hop stacking**

More advanced routes stack steps across several networks:

- DEX swap on one chain,
- bridge to another,
- DEX swap again,
- move into a new wallet cluster,
- repeat.

The point is to stretch the trail across more tools and more domains, increasing the time and cost needed to reconstruct the path.





## 2.7 Stablecoins as laundering rails: settlement speed, liquidity, issuer controls, freezes

Stablecoins have become a preferred medium for many illicit transfers because they combine global movement with low volatility and deep liquidity. Chainalysis reports that stablecoins account for a large share of illicit transaction volume in recent years, in line with broader adoption.

### Why stablecoins are attractive in practice

- Stable units make bookkeeping easier for cross-border groups.
- Fast settlement supports rapid dispersal and cash-out.
- Stablecoins are widely usable across centralized venues and DeFi.
- On low-fee networks, stablecoins support micro-splitting at scale.

FATF's targeted update flags rising stablecoin use by illicit actors, including DPRK-linked actors and terrorist financiers, and notes layering through anonymity tools and dormant VASP accounts.

**Issuer controls and the freeze-avoidance pattern**

Many fiat-backed stablecoins allow issuers to freeze tokens at certain addresses. That creates a back-and-forth:

- defenders can freeze identifiable balances, sometimes quickly,
- launderers try to reduce time spent holding freezable assets or swap into assets less exposed to issuer action.

Elliptic's stablecoin sanctions typologies discuss issuer freezes as a disruption tool. FATF also notes that issuer models may include freezing or monitoring capabilities and that these models are a focus of policy debate.

Issuer freezes are not hypothetical. Reporting in January 2026 described Tether freezing significant USDT amounts linked to illicit activity and noted cumulative freezing and cooperation claims. These events shape tactics: offenders increasingly route stablecoins through rapid swaps and bridges to reduce freeze exposure rather than holding large stablecoin balances for long periods.

**Stablecoins and sanctions evasion**

Stablecoins also appear in sanctions evasion discussions. Reuters reporting from February 2026 describes US scrutiny of Iran's crypto activity and references claims that USDT is used to bypass restrictions. Other investigations have made similar claims about state-linked stablecoin use. For AML analysis, the practical point is not that every stablecoin transfer is suspicious; it is that stablecoins are a favored transport layer because they work well at scale.

## 2.8 NFT and digital collectibles misuse: wash trading, valuation games, marketplace risks

NFT misuse for laundering is best understood as a niche version of art-market abuse: subjective pricing, thin liquidity, and a story-friendly "sale." This does not mean most NFT activity is illicit. It means the structure can be abused.

**Wash trading and self-dealing**

Wash trading in NFTs involves buying and selling the same item between wallets controlled by the same actor, creating fake volume or creating a "legitimate" sale record. Chainalysis documented measurable wash trading and some illicit links in early NFT markets, and academic work examines the mechanics.

**Valuation games and justification stories**

NFTs can support:

- arbitrary price claims (a token sold at a wildly inflated price),
- layered ownership histories that can be used as a cover story,
- self-purchase through associates, turning dirty crypto into "proceeds of sale."

**Marketplace risks**

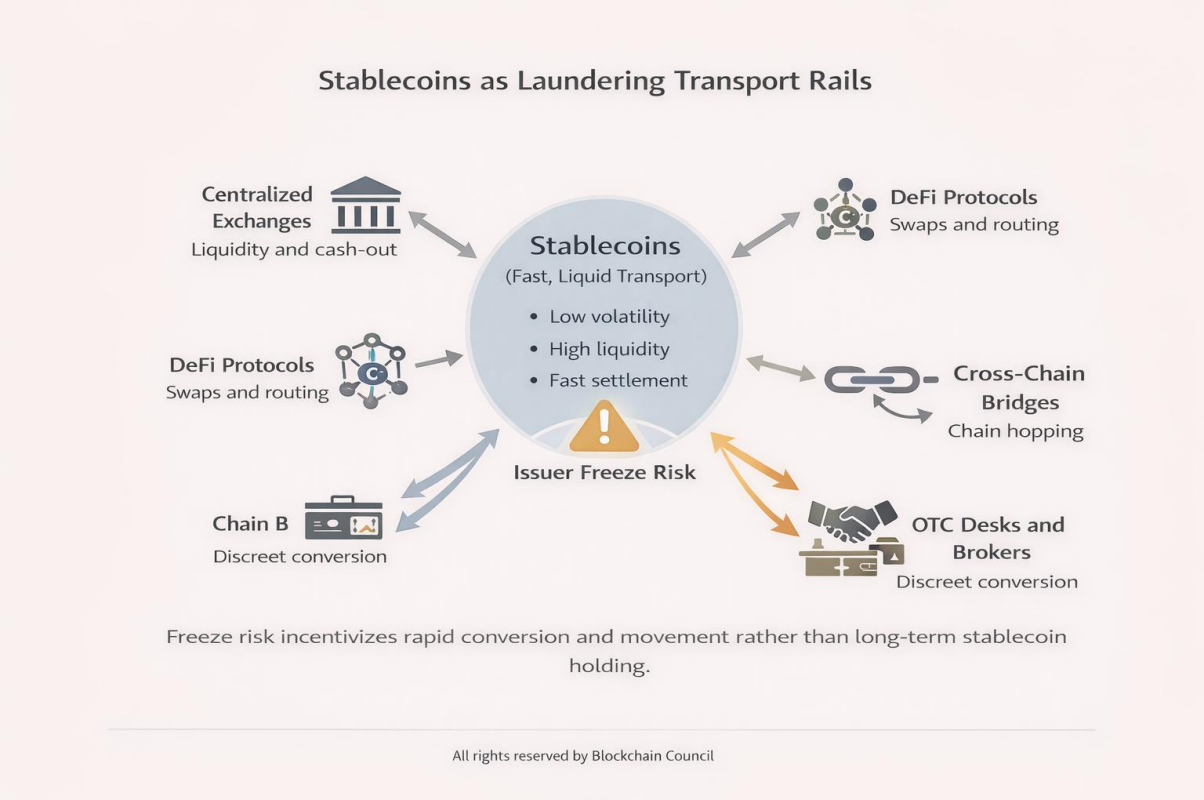
Marketplaces face exchange-like risk issues:

- weak onboarding and identity checks at some platforms,
- exposure to scam-linked inflows,
- difficulty separating genuine collectors from tight wallet circuits.

A practical response is segmentation:

- thin, illiquid segments deserve closer review,

- repeated trades of the same item within a tight wallet cluster are higher risk,
- large-value NFT trades funded by wallets tied to known illicit sources are priority cases.




## 2.9 Crime-linked inflows: ransomware, fraud, scams, darknet markets, sanctions evasion

Laundering routes differ by predicate offense because the starting point differs.

### Scams and fraud as major volume drivers

Scam proceeds are often small per victim but large in total. Chainalysis reported record scam and fraud losses in 2025, estimating $17 billion stolen, driven by evolving impersonation and technology-enabled tactics. These proceeds often enter laundering through victim-directed transfers, then convert quickly into stablecoins and route through laundering networks and OTC channels.

**Industrialized laundering networks and "guarantee platforms"**

A notable 2026 theme is the documented scale of specialist laundering networks, including Chinese-language networks using "guarantee" platforms as escrow-like intermediaries connecting launderers with clients. Reuters reported that crypto money laundering reached at least $82 billion in 2025 and described these networks, including large wallet clusters and high daily processing volumes. Chainalysis separately described these networks and their operating features.

These networks matter because they shift the threat model from "offenders laundering their own proceeds" to "service providers selling laundering at volume."

**Telegram-based black markets and ecosystem support**

Wired reported on the shutdown of Haowang Guarantee (previously Huione Guarantee) following Telegram actions, describing it as a large marketplace for scam infrastructure and laundering services, and

alleging facilitation of tens of billions in illicit transactions. Even when such venues are disrupted, the lesson is consistent: messaging platforms can host service markets that coordinate laundering, and disruptions often drive migration rather than ending demand.

**Darknet markets and fraud shops**

Darknet market inflows rise and fall with takedowns and enforcement. Chainalysis reported that darknet market inflows declined, with DNMs receiving just over $2 billion in BTC on-chain in the period referenced. Laundering routes here often involve peel chains, mixing, and eventual cash-out through exchanges, brokers, or OTC intermediaries.

**Ransomware and stolen funds**

Ransomware proceeds usually start in crypto. The laundering task is to convert those proceeds into spendable value while avoiding detection. National cyber threat reporting continues to treat ransomware as a major risk area, and crypto remains central to ransom payment systems. Common patterns include:

- splitting proceeds across many wallets,
- swapping into stablecoins,
- mixing or CoinJoin for Bitcoin-based proceeds,

- routing through high-risk exchanges or OTC brokers.

**Sanctions evasion and state-linked activity**

Sanctions evasion overlaps with laundering but differs in purpose: preserving access to hard currency, paying for goods, and moving value across restricted boundaries. Reuters reporting in February 2026 on Iran describes large crypto activity and US concern about sanctions evasion via platforms and stablecoins. FATF also flags stablecoin use by DPRK-linked actors and other illicit groups.

## 2.10 Case-study framework: typology selection, indicators, and reproducible mapping

Typologies matter only if researchers can show them in real cases and other teams can replicate the work. This paper uses a mapping approach built around selection criteria, consistent indicators, and clear trace documentation.

**Typology selection criteria**

Case studies should cover:

- different entry routes (kiosks, P2P, exchange-based, crypto-native proceeds),
- different laundering mechanics (peel chains, chain hopping, mixers, DeFi routing, cross-chain bridging),

- different crime sources (scams, hacks, darknet markets, sanctions-linked flows),
- data availability (publicly referenced addresses, court records, sanctions designations, or confirmed exchange seizure records),
- analytic tractability (at least one anchor point that allows some validation).

**Mapping steps (repeatable workflow)**

1. Define the source event: scam cluster, hack, ransomware payment, darknet vendor wallet, or sanctioned entity wallet.
2. Set anchors: sanctions lists, law enforcement seizure disclosures, exchange deposit tags, or published investigative datasets.
3. Trace outward using a consistent hop rule, stopping when: (a) a regulated service is reached, (b) funds enter a mixer, (c) a bridge event occurs, (d) funds fragment beyond a defined threshold, or (e) the time window ends.
4. Tag service interactions: exchanges, OTC brokers, DEX contracts, bridge contracts, mixer contracts, stablecoin issuer interactions.

5. Compute indicators at each stage: hop count, time-to-hop, split ratios, conversion counts, cross-chain transitions, and concentration (how much returns to a cluster).
6. Validate with off-chain sources where possible: court filings, press releases, public reporting, or confirmed service actions.
7. Record uncertainty: probabilistic attribution, ambiguous contract behavior, and incomplete cross-chain visibility.

This mirrors the direction of modern crypto crime research: use on-chain analytics to form testable hypotheses, then seek off-chain validation and state limits clearly.

### 2.11 Red flags and measurable indicators: wallet behavior, counterparty risk, structuring signals

Red flags are useful only when they can be implemented. In crypto AML, the most useful indicators combine behavior (what a wallet does) with context (who it touches). FATF has published red flag indicators drawn from case studies. AUSTRAC provides sector-specific suspicious activity indicators for digital currency businesses. FinCEN's kiosk notice adds channel-specific indicators and risk themes for cash-to-crypto abuse.

#### A. Wallet behavior indicators

- **New wallet rapid activation:** a wallet first seen receiving high-risk inflows, then dispersing quickly.
- **High split ratio:** a large incoming amount breaks into many smaller outputs soon after receipt.
- **Peel chain signatures:** repeated pattern of sending most funds forward while peeling smaller amounts to other addresses or services.
- **Burst-and-dormancy cycles:** a spike after receipt, long inactivity, then renewed movement.
- **Hop stacking:** many hops through contracts and wallets with little time between them.

**B. Counterparty and exposure indicators**

- contact with known-risk services (unlicensed or high-risk exchanges, laundering hubs, sanctioned entities),
- mixer contact (sending to or receiving from mixers), especially when followed by exchange deposits,
- CoinJoin patterns paired with other risk signals,
- frequent bridge use, especially right after high-risk inflows and paired with DEX aggregators,

- stablecoin freeze avoidance: rapid conversion out of freezable stablecoins into other assets or cross-chain moves after publicity or enforcement activity.

**C. Structuring and transaction design indicators**

- threshold-aware structuring: repeated sizes just below known monitoring limits (exchange limits, kiosk limits, internal rules),
- round-trip swaps that repeatedly lose value, suggesting cover rather than trading,
- excessive asset switching without market reason,
- many-to-one reconsolidation: many small inflows from unrelated wallets consolidating into a hub (common in laundering services).

**D. Channel-specific indicators for kiosks and mule-linked placement**

- frequent kiosk purchases by the same customer or linked customers over short periods,
- funds received from many unrelated bank accounts, then used quickly to buy crypto or sent to an exchange,
- victim-directed patterns consistent with scam scripts (urgency, instructions to convert cash to crypto, immediate forwarding).

### E. Risk scoring principles

No single indicator should decide a case. Practical programs:

- combine indicators into typology scores (for example: chain hopping + mixer contact + rapid cash-out attempts),
- weight by source risk (sanctioned entity vs unknown wallet),
- treat speed as a triage factor (fast movement often needs faster action),
- add off-chain context (customer profile, geography, device anomalies, prior SAR history).

### Macro context for 2026

Typologies are scaling up. TRM Labs estimates illicit wallets received $158 billion in incoming value in 2025, a sharp increase from 2024, pointing to renewed growth and more organized activity. Reuters reporting also describes continuing growth in specialist laundering networks and large crypto laundering totals. Across major research and enforcement narratives, the direction is consistent: laundering is not fading; it is becoming more organized.

Taken together, the typologies in this chapter point to one simple reality: crypto laundering functions like a supply chain. Entry routes supply tainted value. Layering methods reshape it and spread it.

Service markets and protocols provide logistics. Exit channels deliver spendable outcomes. The rest of the paper builds on that supply-chain view because it is the only way to evaluate intervention points without relying on slogans.

**Chapter 3: Detection, Regulation, and Enforcement Responses**

Crypto AML/CFT in 2026 is not about proving crime exists. It is about whether regulators and institutions can (1) spot risk early enough to act, (2) make enough choke points cooperate, and (3) do it across borders without creating gaps that offenders can route around or getting stuck on mismatched data rules.

The compliance toolkit now blends familiar controls (customer checks, monitoring, reporting, sanctions screening) with crypto-specific controls (address and wallet screening, on-chain exposure analysis, Travel Rule messaging, smart-contract and bridge monitoring, and coordination around stablecoin freezes). The same tools that let criminals move value faster can also help defenders move faster—when there is an accountable intermediary and supervisors can enforce basic standards.

This chapter explains what intermediaries are required to do in practice, how Travel Rule compliance works day to day, which regulatory models shape the sector through 2026, and what enforcement has actually done. It also covers the hard cases (DeFi and

self-hosted wallets), forward risks (more automation and AI-enabled laundering), and a set of metrics for judging whether controls change outcomes.

### 3.1 Compliance duties in practice: KYC/CDD, ongoing monitoring, STR/SAR triggers, recordkeeping

In jurisdictions that regulate virtual asset activity in a meaningful way, crypto-asset service providers (CASPs in the EU) and virtual asset service providers (VASPs in FATF terms) are treated as obliged entities. Their duties broadly mirror those of other financial institutions. FATF states the baseline plainly: VASPs should be subject to relevant FATF measures, applied using a risk-based approach.

#### A. KYC and CDD: identity, beneficial ownership, and customer risk profiling

CDD in crypto has two layers: who the customer is and what the customer's activity looks like on-chain. Strong programs join both into one customer risk view.

Core identification steps usually include:

- **Natural persons:** name, date of birth, address, an identification number, and verification using reliable independent sources.

- **Legal persons:** legal name, registration details, beneficial owners (where required), controlling persons, and checks against registries and supporting documents.
- **Purpose of the relationship:** products used (spot, derivatives, custody, staking, OTC), expected volumes, source of funds and wealth, and geography.

Crypto-specific additions often include:

- **Wallet association:** recording customer deposit and withdrawal addresses and linking them to the customer profile so they can be monitored over time.
- **Proof of control (when required):** showing that a customer controls a self-hosted address (for example, message signing, small confirmation transfers, or third-party attestations). EU rules anticipate ownership or control checks for self-hosted addresses above a threshold (discussed in 3.2 and 3.10).
- **Source-of-funds and source-of-wealth checks informed by on-chain context:** exposure to high-risk services, mixers, sanctioned entities, scam clusters, ransomware-linked clusters, and high-risk jurisdictions.

CDD is not a one-time gate. Updates are triggered by changes in behavior, adverse media, sanctions updates, sharp volume changes, or

new product use (for example, shifting from spot trading into frequent bridge use and DeFi routing).

**B. Enhanced due diligence: where programs either add friction or do not**

EDD is where institutions either slow laundering or create paperwork that does not matter. EDD commonly applies to:

- **Higher-risk customers:** politically exposed persons, higher-risk geographies, complex ownership, high-value customers with unclear wealth.
- **Higher-risk channels and tools:** mixers and other privacy tooling, higher-risk OTC activity, frequent bridge use, and heavy use of self-hosted wallets.
- **Higher-risk patterns:** rapid in-and-out flows, chain hopping, structuring, and behavior that matches known typologies.

Within the EU Travel Rule setting, transfers involving self-hosted addresses create explicit expectations for risk management, including EBA guidelines and Commission review duties (see 3.2 and 3.10).

**C. Ongoing monitoring: transaction monitoring in a cross-chain world**

Ongoing monitoring in crypto merges account activity with blockchain analytics. Programs tend to develop from simple rule sets into mixed systems that use rules, behavior baselines, and graph-based exposure.

Common elements include:

- **Rules and thresholds:** large deposits or withdrawals, velocity rules, repeated near-threshold activity, rapid conversions, and high-risk counterparty hits.
- **Behavior analytics:** spotting deviations from a customer's usual pattern (frequency, assets used, typical counterparties).
- **On-chain exposure scoring:** graph-based exposure to illicit clusters, mixers, sanctioned entities, and risky services.
- **Smart-contract interaction monitoring:** identifying contact with known-risk contracts, bridges, DEX routers, and other laundering infrastructure.
- **Cross-chain tracing:** tracking equivalent value through bridges and wrapped assets. This matters because chain hopping is now routine in many laundering routes.

The day-to-day problem is triage. Teams cannot investigate everything. The quality of prioritization and the control of false positives often matter as much as detection.

### D. STR/SAR triggers: turning suspicion into a reportable event

Suspicious transaction reports (STRs) or suspicious activity reports (SARs) remain a core AML output. Crypto reporting logic usually combines several factors:

- **Known-risk exposure:** direct or close contact with sanctioned addresses, ransomware wallets, scam clusters, darknet market clusters, or mixers.
- **Typology fit:** behavior consistent with placement, layering, and exit patterns described in Chapter 2.
- **No plausible explanation:** activity that conflicts with the customer's stated purpose, business model, or normal behavior.
- **Evasion signals:** structuring, rapid hop stacking, use of obfuscation tools after receiving suspicious inflows, and attempts to bypass controls.

Many regimes also require separate reporting of sanctions hits or blocked property events where targeted financial sanctions apply.

### E. Recordkeeping: why it matters in crypto

Recordkeeping is the bridge between an on-chain trail and a real-world person. Without it, investigations stall, and institutions cannot support lawful requests quickly.

Key records include:

- identity and verification documents,
- transaction records (timestamps, amounts, assets, counterparties),
- Travel Rule messages and related metadata where applicable,
- wallet addresses linked to customers, including changes over time,
- internal compliance records: alerts, notes, decisions, and SAR/STR filings.

In the United States, recordkeeping and Travel Rule duties for funds transmittals appear in Bank Secrecy Act rules such as 31 CFR 1010.410, which sets retention requirements for transmittals above a stated threshold.

### 3.2 Travel Rule implementation for crypto transfers: required data, messaging, operational drag

The Travel Rule is the attempt to make crypto transfers resemble traceable wire transfers when intermediaries are involved. It requires originator and beneficiary information to accompany transfers between regulated entities. FATF treats this as a payment transparency expectation, and weak implementation remains a recurring gap.

### A. Required data: originator and beneficiary information

Details vary by country, but common data fields include:

- **Originator:** name, account or wallet identifier, and additional identifying information such as address, national ID, customer ID, or date of birth depending on thresholds and local rules.
- **Beneficiary:** name and account or wallet identifier.

FATF's 2025 updates to Recommendation 16-related materials reinforced a EUR/USD 1,000 threshold for required information in certain contexts, continuing the push toward consistent payment transparency requirements.

The EU has one of the broadest approaches for crypto transfers. Regulation (EU) 2023/1113 extends transfer-information requirements to crypto-asset transfers when a CASP is involved, including transfers to or from self-hosted addresses where a CASP touches the flow.

### B. EU Travel Rule specifics: scope and self-hosted addresses

Under Regulation (EU) 2023/1113, CASPs must collect originator and beneficiary information for crypto-asset transfers when they are involved, including when the counterparty is a self-hosted address.

A key line is drawn at EUR 1,000 for certain verification expectations:

- For transfers above EUR 1,000 to or from a self-hosted address, the CASP should take steps to assess whether the address is owned or controlled by its client.

The Commission must assess risks from transfers involving self-hosted addresses and consider additional mitigation measures, with a report due by 1 July 2026.

EBA guidelines under this regime apply from 30 December 2024 and set expectations for policies, procedures, and the handling of transfers where required information is missing or deficient.

**C. Messaging infrastructure: standards and interoperability**

Travel Rule compliance is a plumbing problem as much as a policy problem. CASPs/VASPs need secure channels to exchange identity data while keeping confidentiality and data integrity.

IVMS 101 (interVASP Messaging Standard 101) is widely used as a shared data format for Travel Rule fields to reduce incompatibility across solution providers.

In practice, institutions use:

- Travel Rule solution providers and networks that exchange IVMS 101 messages,
- direct integrations between major exchanges and custodians,

- fallback processes when counterparties are not on the same network, which increases delay and risk.

**D. Why implementation remains uneven**

Even with rules in place, practical frictions are predictable:

- **Coverage gaps:** the Travel Rule works best when both sides are regulated and able to send and receive compliant messages. Uneven cross-border adoption weakens coverage, and FATF updates repeatedly flag this.
- **Self-hosted wallets:** there is no built-in identity layer. "Assessing ownership or control" above a threshold is required in the EU setting, but proving control at scale without blocking legitimate use is hard.
- **Data protection and security:** sending identity data raises privacy and breach risk. In the EU, GDPR duties can collide with a simple "send more data" instinct.
- **Speed and user expectations:** users expect fast deposits and withdrawals. Travel Rule steps add error handling and sometimes manual review.
- **Error management:** mismatched names, missing fields, and weak identifiers create false stops and manual queues. EBA

guidelines address how to detect and manage missing or deficient information because this is common in practice.

### 3.3 Regulatory models in 2026: licensing, supervision, and cross-border reality

Crypto AML/CFT regimes through 2026 broadly fall into several models:

- **Registration-based:** basic registration as an obliged entity with AML duties, sometimes with limited broader supervision.
- **Licensing-based:** authorization to provide crypto-asset services, with governance, capital, conduct, and AML requirements.
- **Restrictive models:** tight limits on retail access or specific products (for example privacy assets or derivatives), which can push activity offshore.
- **Hybrid models:** different requirements depending on service type (custody, exchange, issuance, transfers).

The structural problem is cross-border mismatch. Crypto is borderless. Supervision is not. FATF continues to warn that weak implementation in one place can spill over globally, and its reviews show many countries still lag.

Cross-border enforcement realities in 2026 include:

- **Jurisdiction shopping:** high-risk services and illicit operators choose places with weak oversight.
- **Long-arm pressure:** major jurisdictions, especially the US and EU, exert influence through sanctions, banking access pressure, and prosecution of services that touch their markets.
- **Joint actions:** more coordinated takedowns where services have identifiable operators or infrastructure (see 3.8).
- **Fragmented rules for DeFi and self-hosted wallets:** where accountability is unclear, enforcement slows and ambiguity becomes a tool.

### 3.4 European Union framework: CASP authorization, token issuer rules, transfer-information regime

Through 2026, the EU framework relevant to this paper rests on three pillars: MiCA for market and service rules, the transfer-information regime for crypto transfers, and the wider AML package including the new EU AML Authority.

#### A. MiCA: authorization and conduct rules

MiCA (Regulation (EU) 2023/1114) sets an EU-wide framework for crypto-asset issuance and services. It applies from 30 December 2024, with stablecoin-related provisions applying earlier from 30 June 2024.

For AML purposes, MiCA matters because it:

- defines regulated crypto-asset services and duties for providers,
- allows authorization and passporting across the EU, reducing internal regulatory arbitrage,
- imposes requirements on token issuers, especially for asset-referenced tokens and e-money tokens (stablecoin categories), which intersects with stablecoins' role in laundering routes.

MiCA also continues to be shaped by technical standards and supervisory guidance, including ESMA implementation materials.

**B. Transfer-information regime: Regulation (EU) 2023/1113**

Regulation (EU) 2023/1113 extends transfer-information requirements to crypto-asset transfers when a CASP is involved. It covers transfers to and from self-hosted addresses where a CASP touches the transfer and includes:

- the EUR 1,000 expectation to assess ownership or control of self-hosted addresses, and
- the Commission risk review with a report due by 1 July 2026.

EBA guidelines specify how to deal with missing or deficient information and how to manage risk when required information is incomplete.

### C. EU AML package and AMLA: consolidation underway

The EU adopted a major AML package in 2024, including Regulation (EU) 2024/1624 (applying from 10 July 2027, with limited exceptions) and the creation of AMLA under Regulation (EU) 2024/1620.

Although the AML Regulation applies in 2027, the direction matters through 2026 because firms are already preparing and AMLA is building capacity. Reuters reporting in February 2026 described AMLA's plan and timeline toward being fully operational in 2028, including direct supervision of selected higher-risk institutions and attention to risks such as crypto-assets.

The strategic point for crypto AML is that EU supervision is moving from fragmented national approaches toward more consistent risk-based oversight inside the EU, even though global gaps remain outside it.

## 3.5 United States framework: BSA/FinCEN approach, sanctions tools, focus on higher-risk services

In the United States, crypto AML/CFT is driven by the Bank Secrecy Act, FinCEN rules and guidance, sanctions enforcement by OFAC, and criminal enforcement by DOJ and others. The US approach is

marked by aggressive use of enforcement against intermediaries that serve US users or touch US systems.

**A. BSA duties and the funds-transfer recordkeeping Travel Rule baseline**

The US Travel Rule concept appears in BSA recordkeeping rules for transmittals of funds above $3,000, including retention and transmission of key sender and recipient information.

Crypto businesses treated as money services businesses generally must run AML programs, perform customer identification where required, keep records, and file SARs. The framework focuses accountability on intermediaries that custody or transmit value.

**B. FinCEN focus on higher-risk services: mixing as a priority concern**

FinCEN proposed a Section 311 special measure rulemaking in October 2023 to designate international convertible virtual currency mixing as a class of transactions of primary money laundering concern. The proposal would add reporting and recordkeeping duties for covered institutions for transactions involving such mixing.

Even as a proposal, the message is clear: US policy treats mixing as a major enabler and tries to address it through added reporting and pressure on institutions to identify and report related activity.

### C. Sanctions tools: OFAC expectations and the mixer sequence

OFAC has issued sanctions compliance guidance for the virtual currency sector, stressing risk-based compliance, screening, recordkeeping, and reporting.

Sanctions have been used against mixers and laundering facilitators. OFAC sanctioned Sinbad in November 2023, alleging it supported laundering tied to DPRK-linked activity.

The Tornado Cash episode shows a legal constraint. A US appeals court overturned OFAC's 2022 Tornado Cash sanctions in late 2024 on grounds tied to the legal status of immutable smart contracts. Treasury removed Tornado Cash from the sanctions list in March 2025 while reiterating concern about DPRK-linked laundering.

The lasting lesson for 2026 is practical: sanctions attach more cleanly to identifiable operators, interfaces, and service providers than to decentralized code without a controllable owner. Enforcement pressure shifts toward intermediaries.

### D. Enforcement examples: exchanges and infrastructure

US enforcement has increasingly targeted exchanges and services alleged to support laundering or evade licensing requirements.

- **Garantex disruption (2025):** DOJ described a coordinated action with Germany and Finland to disrupt Garantex, alleging

money laundering and sanctions violations and citing large transaction volumes.

- **OKX operator guilty plea (2025):** Reuters reported that Aux Cayes FinTech Co, operator of OKX, pleaded guilty to violating US AML laws and agreed to substantial penalties and compliance monitoring, with allegations of large suspicious transaction volumes and evasion of US user restrictions.

These cases illustrate a core US tactic: use licensing and AML failures (including unlicensed money transmission) to force program changes and discourage servicing high-risk flows.

**E. Enforcement capacity shifts: changes in prioritization**

Enforcement intensity changes with budgets and priorities. AP reported in 2025 that DOJ would disband its National Cryptocurrency Enforcement Team and shift focus toward crimes where crypto is a tool (fraud, trafficking, terrorism) rather than pursuing complex regulatory violations as a primary goal.

For AML outcomes, these shifts matter because they influence deterrence and how likely compliance failures are to face serious consequences.

**3.6 FATF-driven convergence and gaps: uneven adoption, regulatory arbitrage, supervisory capacity**

FATF remains the global coordination layer. Its standards shape shared scope and expectations: licensing or registration of VASPs, risk-based AML/CFT programs, and Travel Rule implementation.

**A. What convergence looks like**

Common points of convergence include:

- licensing or registration of VASPs/CASPs,
- program requirements for CDD, monitoring, and reporting,
- Travel Rule duties for originator and beneficiary information exchange,
- growing attention to stablecoins, cross-chain flows, and DeFi-related gaps.

FATF's 2025 targeted update flags increased stablecoin use by illicit actors and notes that criminals layer using anonymity tools and dormant VASP accounts, while DeFi oversight remains difficult.

**B. What gaps look like in 2026**

Gaps persist in at least three forms:

- **legal adoption gaps:** jurisdictions that have not adopted VASP regulation or Travel Rule rules,
- **supervisory capacity gaps:** laws exist on paper but supervision and enforcement are weak,

- **interoperability gaps:** Travel Rule messaging and coordination remain fragmented, especially cross-border.

Reuters reporting on FATF's June 2025 update noted that only a minority of assessed jurisdictions were described as "largely compliant," showing the difference between standards and real-world uptake.

### C. Regulatory arbitrage and leakage

Illicit flows route around controls. When one jurisdiction tightens supervision, flows shift to less supervised exchanges, OTC networks, and cross-chain paths. This leakage is why FATF stresses borderless risk and why EU and US enforcement increasingly targets cross-border services that support laundering at scale.

## 3.7 Blockchain analytics: capabilities, common heuristics, false positives, adversarial response

Blockchain analytics supports much of crypto AML monitoring, but it is not magic. It draws probabilistic inferences from public ledgers and often needs off-chain data to connect addresses to real people.

### A. What analytics can do well

- **Tracing on public ledgers:** follow value through addresses and contracts, identify service contact, and map transaction graphs.

- **Entity clustering:** infer that address sets likely belong to the same actor using heuristics (common-input and change behavior for UTXO systems; behavior and contract-contact patterns for account-based chains).
- **Exposure scoring and typology detection:** spot patterns such as peel chains, mixer contact, rapid chain hopping, and bridge use.
- **Intelligence fusion:** integrate sanctions lists, seizure disclosures, and known illicit clusters.

BIS analysis points to the core AML opportunity: many blockchains allow tracing and monitoring that is far harder in cash-heavy systems. BIS also notes that measured illicit volumes (for example, $51.3 billion in 2024) are likely lower bounds and depend on attribution quality.

**B. Why heuristics create errors**

Heuristics are necessary because an address is not a legal identity. But inference creates both false positives and false negatives.

Examples include:

- **multi-input clustering risks:** on UTXO systems, the common-input heuristic can miscluster CoinJoin activity or shared custody structures,

- **single-heuristic failure:** research notes that relying on one heuristic often produces weak clustering and supports multi-heuristic approaches.

In practice, programs reduce error by:

- requiring multiple signals before action (exposure plus behavior plus counterparty risk),
- separating “risk scoring” from “identity certainty,” treating many analytic results as leads,
- keeping audit trails and human review for high-impact decisions (account closure, freezes).

**C. How offenders exploit analytic limits**

Chapter 2 listed the tactics. The point here is their effect on monitoring:

- chain hopping and bridges force analysts across multiple tool stacks and data sources,
- aggregators and swap routers create dense traces with little added attribution value,
- self-hosted wallets reduce identity anchors,
- mixers and privacy tools reduce or destroy linkability.

Enforcement actions against mixers and laundering services (including takedowns supported by Europol, such as Cryptomixer) show that institutions treat these tools as major drivers of investigative cost.

### 3.8 Investigations and enforcement: subpoenas, seizures, sanctions listings, international coordination

Crypto investigations combine classic financial investigation tools with on-chain tracing.

#### A. Subpoenas and compelled records: how attribution often happens

Even strong tracing often becomes conclusive only when investigators compel records from intermediaries:

- exchange records (KYC files, deposits and withdrawals, IP logs, device fingerprints, linked bank accounts),
- payment records tied to fiat gateways (bank transfers, cards, payment-app logs),
- infrastructure records (hosting providers, domain registries, and other service providers for illicit sites).

Where offshore services refuse cooperation, cases slow down and depend more on cross-border legal assistance.

### B. Seizures and freezes: disruption on token rails

Common disruption tools include:

- seizure warrants for private keys or custodial accounts,
- stablecoin issuer freezes (where issuer controls exist),
- takedowns of infrastructure, operator arrests, and domain seizures.

US and European actions against exchanges and mixing services illustrate these approaches. DOJ's Garantex action described international coordination. Europol's action-week approach for Cryptomixer shows similar cross-border tactics.

### C. Sanctions listings: designations as a private-sector trigger

Sanctions listings push duties onto the private sector. Once an address or entity is listed, regulated intermediaries must block or restrict activity and report as required. OFAC guidance for the virtual currency sector sets expectations for screening, reporting, and records.

The Tornado Cash sequence also shows the political and legal sensitivity of sanctions applied to decentralized tools, including delisting in 2025 after legal challenges and an appeals court ruling.

### D. International coordination: more operational, still limited

Coordination includes:

- mutual legal assistance and joint investigation teams,
- Europol and Eurojust support for EU-wide cases,
- FIU information sharing.

The EU's longer-term bet is AMLA, intended to improve supervisory consistency and cross-border response capacity on a timeline toward 2028.

### 3.9 Industry controls: exchange screening, wallet risk scoring, smart-contract monitoring, limits

Industry controls are the first line of defense when they are more than paperwork.

#### A. Exchange and custodian controls

Common controls include:

- sanctions screening for addresses and customers,
- wallet risk scoring based on exposure to illicit clusters, mixers, ransomware, scams, and sanctioned entities,
- transaction monitoring with holds and manual review,
- limits and tiering based on verification level, geography, and behavior.

Enforcement outcomes often drive upgrades. Reuters reporting on the OKX operator resolution included a requirement for an external compliance consultant through at least 2027, a common enforcement tool used to push program change.

**B. Smart-contract and DeFi monitoring**

Institutions increasingly monitor:

- contact with known-risk contracts (mixers, exploit contracts, laundering routers),
- bridge use and cross-chain activity,
- DeFi patterns consistent with layering (swap chains, lending loops).

Treasury's DeFi risk assessment stresses gaps in accountability across DeFi layers (application, interface, settlement), implying that monitoring must occur at multiple layers rather than assuming protocols sit outside view.

**C. Travel Rule operational controls**

Common practices include:

- exchanging Travel Rule messages using standardized fields (IVMS 101),
- counterparty checks for foreign VASP/CASP relationships,

- exception handling where counterparties cannot receive compliant messages.

**D. Limits and de-risking**

Some providers reduce exposure by restricting services:

- limiting support for privacy tools or higher-risk assets,
- blocking or limiting contact with certain chains or bridges,
- applying added checks for withdrawals to self-hosted addresses above thresholds.

These steps can reduce exposure at one firm while pushing activity to less supervised venues, which is why cross-border consistency still matters.

### 3.10 The hard problems: DeFi accountability, self-hosted wallets, privacy rights vs crime control

Some problems do not yield to "do more KYC."

**A. DeFi accountability**

DeFi protocols do not always have a clear operator who can run AML controls, and settlement is often decentralized. Treasury notes that illicit actors exploit gaps where duties are unclear or absent and that accountability differs across layers such as interfaces and application operators.

Practical implications include:

- enforcement focusing on identifiable intermediaries: front-end operators, developers where legally reachable, bridge operators, and centralized entry/exit services,
- compliance focusing on junctions where DeFi meets intermediaries: exchange withdrawals into DeFi, issuer controls for stablecoins, and bridge services.

Protocol-level AML duties remain contested and hard to enforce when code is immutable or governance is diffuse.

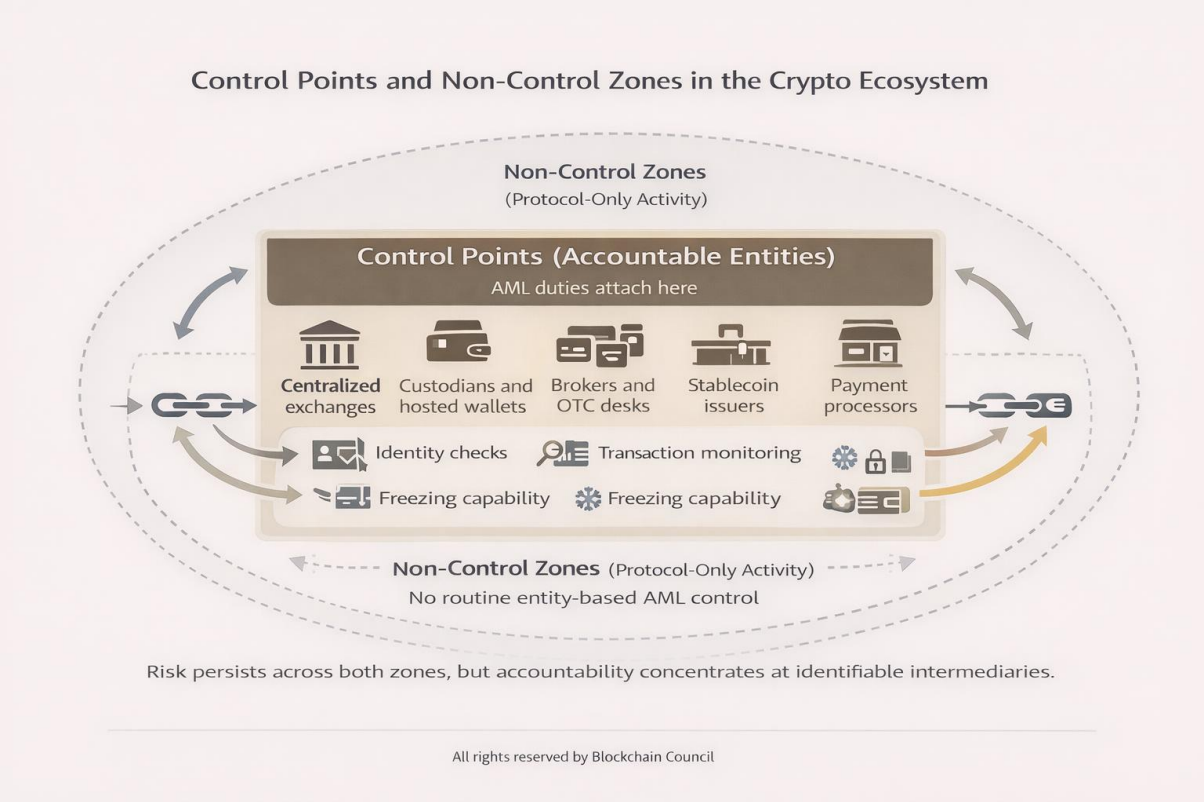
**B. Self-hosted wallets: autonomy versus traceability**

Self-hosted wallets serve legitimate needs: privacy, self-custody, and security. They also serve laundering because there is no built-in identity layer.

EU rules put this tension into law:

- transfers involving self-hosted addresses fall within Regulation (EU) 2023/1113 when a CASP is involved,
- above EUR 1,000, CASPs should assess whether the self-hosted address is owned or controlled by their client,
- the Commission must assess risks and consider further measures by 1 July 2026.

This makes self-hosted wallets a live policy issue through 2026 because regulators must define what "ownership verification" means technically and how to avoid turning it into either a box-tick exercise or a de facto ban on self-custody.




## C. Privacy rights and the limits of sanctions against code

The Tornado Cash sequence is a concrete example:

- sanctions imposed in 2022,
- an appeals court decision in late 2024 overturning the sanctions on legal grounds tied to immutable smart contracts,

- Treasury delisting in March 2025 while stressing continued concern about illicit use.

The constraint is durable: enforcement tools work best when there is a clear target with property interests that can be controlled. When the tool is decentralized code, pressure shifts to operators, interfaces, facilitators, and downstream intermediaries.

### 3.11 Forward risks (2026): AI-enabled laundering, new obfuscation patterns, scaling

The forward risk is not a wholly new set of techniques. It is the scaling of known techniques until monitoring and investigation capacity is overwhelmed.

#### A. Automation of micro-structuring and dispersal

Offenders already split funds, chain hop, and use timing tricks. With more automation, these behaviors can run continuously and adjust in response to controls. Discussions of "agentic smurfing" describe autonomous systems running micro-laundering at scale, outpacing detection tuned to fixed thresholds and simple rules.

#### B. AI-enhanced fraud as the upstream driver

Europol has warned that AI and related tools can increase the reach and speed of criminal operations, especially in cyber-enabled fraud and scams. These crimes feed laundering pipelines when victims are

pushed into crypto transfers or when proceeds are converted into stablecoins and moved offshore.

**C. Scaling signals in 2025 to early 2026 reporting**

Threat reporting continues to show large volumes. TRM Labs' 2026 crypto crime report estimates illicit crypto volume reached $158 billion in 2025, while noting that illicit volume as a share of total volume can fall even as absolute volume rises.

FATF continues to flag growth in stablecoin use by illicit actors and ongoing difficulty supervising DeFi-related arrangements.

**D. Likely obfuscation trends**

Based on observed adaptation patterns, likely trends include:

- more cross-chain hop stacking to break tracing continuity,
- faster stablecoin-to-native conversions to reduce exposure to issuer freezes,
- heavier use of aggregators and routing contracts to increase transaction complexity,
- more laundering-as-a-service markets migrating across communication platforms and surviving takedowns through replication.

### 3.12 Research gaps and a proposed evaluation framework: effectiveness metrics for crypto AML

The field has plenty of debate and too few comparable outcome measures. A useful evaluation approach separates (1) detection, (2) disruption, and (3) deterrence, while accounting for false positives, false negatives, and displacement (crime shifting elsewhere).

#### A. Research gaps through 2026

- **Limited ground truth:** most on-chain attribution is probabilistic; confirmed labels are largely limited to law enforcement releases, sanctions lists, and cooperative exchange cases.
- **Cross-chain measurement:** methods for following value across bridges and wrapped assets vary across tools and studies.
- **False positive measurement:** academic work notes heuristic error risk, but operational settings rarely publish error rates.
- **DeFi accountability measurement:** few studies measure whether interventions (front-end blocks, stablecoin freezes, bridge interdiction) reduce illicit throughput.
- **Travel Rule impact:** implementation can be measured (coverage, latency, error rates), but links to reduced laundering are still under-studied.

## B. Evaluation framework: metrics that can be reported and compared

The metrics below are designed for researchers and supervisors and do not require access to proprietary exchange internals, though deeper data improves accuracy.

### Coverage metrics

a) **Regulated touchpoint coverage:** share of observed high-risk flows that touch a regulated intermediary at any point (exchange, custodian, issuer, OTC desk).

b) **Travel Rule coverage:** share of CASP-to-CASP transfers that include complete required fields, broken down by corridor and asset type.

c) **Cross-chain trace continuity:** share of bridged flows where equivalent value can be followed across chains with high confidence.

### Detection metrics

a) **Alert precision:** share of alerts that lead to substantiated cases (internal confirmation, SAR/STR filing, or law enforcement referral).

b) **Estimated recall:** share of known illicit flows from labeled sources (sanctions, seizures, public cases) that the system flags.

c) **Time-to-detection:** time between first suspicious inflow and first compliance intervention (alert, hold, SAR).

**Intervention and disruption metrics**

a) **Time-to-freeze or block:** time from identification to action for stablecoin issuer freezes or exchange interdictions.

b) **Recovery rate:** value frozen or recovered divided by estimated illicit value moving through the monitored population.

c) **Chokepoint conversion rate:** share of traced illicit flows that reach an accountable service capable of interdiction.

**Reporting quality metrics**

a) **SAR/STR quality scoring:** completeness, specificity, typology mapping, inclusion of addresses and transaction IDs, and cross-chain narrative quality.

b) **Feedback loop rate:** share of SARs that receive law enforcement feedback or generate follow-up requests.

**Cost and harm metrics**

a) **False positive burden:** manual review time per true positive, user friction incidents, and account closures later reversed.

b) **Displacement index:** whether interdicted flows reappear via other services or chains, indicating migration rather than reduction.

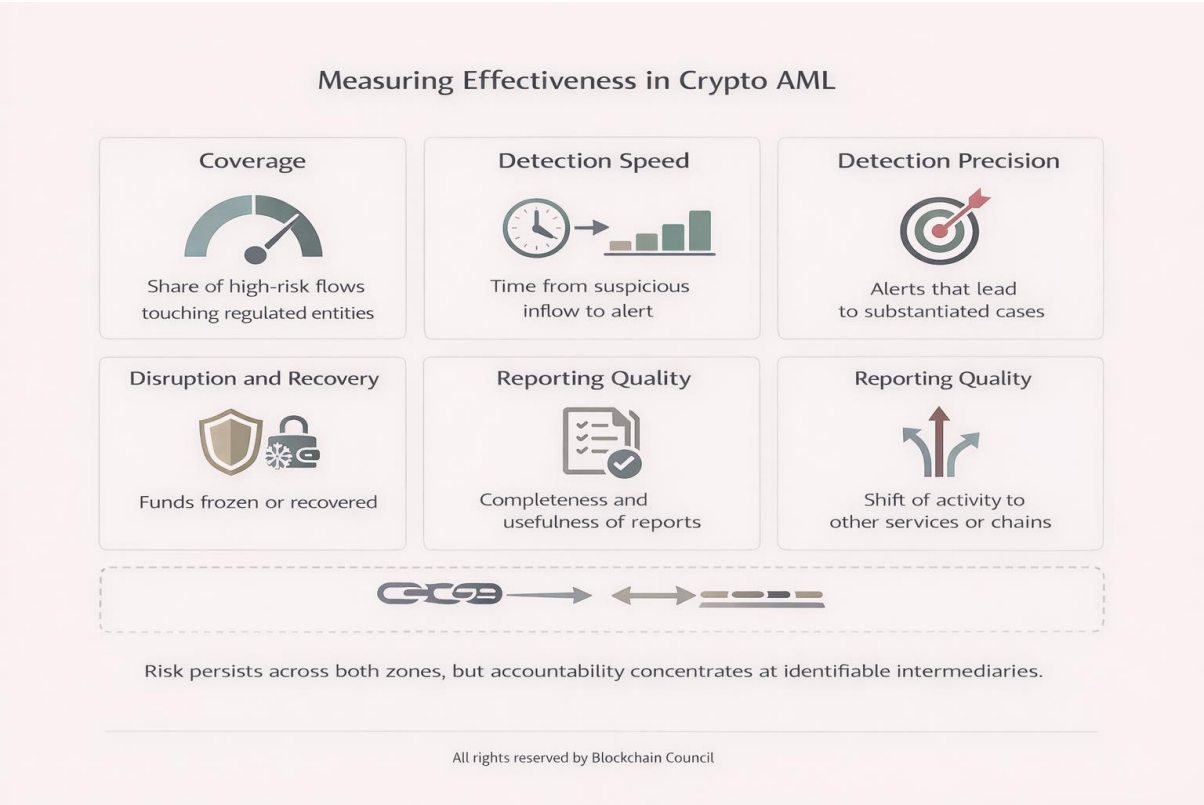
### C. Suggested methods for researchers

- start from labeled anchors (sanctions, official press releases, court filings),
- state uncertainty clearly (confirmed, likely linked, unattributed but behaviorally similar),
- publish trace rules (hop limits, bridge identification rules, clustering heuristics),
- keep policy claims separate from measurement (a control existing is not the same as a control reducing laundering).

### D. What success looks like in crypto AML

Success is not eliminating laundering. Success is shrinking the set of liquid, low-friction laundering routes by raising cost, time, and the chance of disruption.

Through 2026, the direction is clear: more licensing, more transfer information duties, wider use of analytics, and more targeted action against facilitators. The open question is whether these measures reduce laundering in absolute terms or mostly push it into a more fragmented, more automated, and harder-to-supervise set of routes. That is why this field needs metrics rather than slogans.




## Conclusion

Crypto-assets have become a durable part of the money laundering landscape because they provide fast settlement, global reach, deep liquidity in major assets and stablecoins, and a fragmented ecosystem that enables jurisdiction shopping. Yet the most important driver of laundering advantage is not invisibility. It is the gap between traceability and attribution. Public ledgers can preserve transaction histories while leaving the controlling person unknown. Laundering, therefore, is best understood as a set of operational tactics aimed at severing the link between an observable trail and an identifiable actor,

while still preserving the ability to store, move, and ultimately use value.

This paper has argued that the placement, layering, and integration scaffold remains useful in crypto contexts, but it should not be treated as a rigid pipeline. In many modern cases, proceeds originate in crypto, compressing classic placement and shifting early activity toward dispersal, control, and seizure avoidance. Even where proceeds begin in fiat, placement routes are now diversified, including exchanges and brokers, peer-to-peer markets, kiosks, and mule networks. Layering has expanded through asset hopping, cross-chain movement, and smart-contract based routing that can be executed at scale through automation. Integration continues to cluster around cash-out, spending, and investment, and these moments often remain the most actionable points for identification and interdiction because they intersect with regulated entities, contractual relationships, and real-economy documentation.

A central finding is that crypto laundering in 2026 is best modeled as pathways assembled from building blocks rather than as a single technique. The typologies described in this paper illustrate how offenders mix and match entry routes, wallet behaviors, conversion patterns, cross-chain transitions, and exit channels depending on the predicate offense, the control pressure they face, and the outcome they

seek. Chain hopping and bridge use increase investigative cost by forcing analysis across multiple ledgers and tool stacks. Routers and aggregators increase hop density and ambiguity without requiring bespoke criminal infrastructure. Mixing and privacy-enhancing schemes directly target linkability, while privacy-focused assets reduce on-chain visibility and force greater reliance on off-chain evidence. Stablecoins act as preferred transport rails because they reduce volatility and support rapid dispersal and bookkeeping across borders, even while issuer freeze capabilities create an evolving freeze-avoidance dynamic.

The actor and infrastructure mapping clarifies why effective control points are uneven. Duties attach most cleanly where there is an identifiable legal entity, a customer relationship, and some control over funds or access. Centralized exchanges, brokers, custodians, payment intermediaries, and certain OTC desks can operate conventional compliance programs, including customer due diligence, monitoring, reporting, sanctions screening, and recordkeeping that enables attribution. Stablecoin issuers may have strong intervention capacity through freezing mechanisms, although this concentrates power and does not address assets outside issuer control. In contrast, self-hosted wallets and non-custodial protocols often sit outside routine entity-based duties, shifting the defense model toward

perimeter controls, tracing, targeted enforcement against facilitators, and cross-border investigative capacity.

The discussion of regulatory and enforcement responses highlights both progress and persistent constraints. Risk-based AML programs, Travel Rule messaging, blockchain analytics, sanctions enforcement, and coordinated investigations have all expanded the defensive toolkit. At the same time, coverage gaps remain where cross-border implementation is uneven, where counterparties are outside regulated networks, and where accountability for protocol-layer activity is unclear or contested. These gaps are not theoretical. They shape offender choice and support the migration of illicit flows toward weaker corridors, higher-risk service providers, and more complex cross-chain routes. As enforcement pressure rises on one service type, offenders substitute others. The functional demand for obfuscation persists, and markets for laundering facilitation adapt.

From this analysis, three practical implications follow.

First, the most effective near-term gains come from raising consistency and responsiveness at regulated choke points. That includes stronger onboarding and beneficial ownership controls, monitoring that integrates on-chain exposure with customer context, faster escalation and reporting, and more reliable information exchange where Travel Rule duties apply. These measures increase

attribution probability and reduce the time window in which illicit value can be dispersed.

Second, perimeter and infrastructure strategies matter because large portions of activity occur outside custodial control. Monitoring and disruption need to focus on junctions where self-custody meets services, where cross-chain movement is facilitated, and where stablecoin rails provide identifiable intervention levers. Targeted action against high-impact laundering services, laundering-as-a-service networks, and repeat facilitators can raise system-wide costs more than broad restrictions aimed at ordinary users.

Third, evaluation must move from compliance existence to outcome measurement. Rules, tools, and guidance are not the same as reduced laundering. The proposed metrics framework provides a way to compare programs and policies using observable indicators: the share of high-risk flows that touch accountable intermediaries, the completeness and timeliness of transfer information exchange, time-to-detection and time-to-intervention, recovery and disruption rates, reporting quality, and displacement patterns. Without such measures, it is easy to confuse activity with effectiveness.

The paper also underscores limitations that should temper overconfident claims. On-chain analytics relies on probabilistic inference and is vulnerable to false positives and false negatives,

especially when applied without off-chain corroboration. Cross-chain tracing remains methodologically inconsistent across tools and contexts. Transaction intent is often ambiguous on-chain, and attribution frequently depends on compelled records, cooperation, or investigative breakthroughs. These constraints are precisely why outcome metrics, transparent tracing rules, and clear statements of uncertainty are essential.

In sum, crypto's role in money laundering is neither a temporary anomaly nor a simple problem with a single technical fix. It reflects an ecosystem where value can move quickly and globally, where transaction trails persist, and where identity is selectively exposed. The feasible path forward is pragmatic: tighten and harmonize controls where entities exist, improve cross-border interoperability and response speed, develop targeted disruption capacity for high-impact facilitators, and measure success using outcomes rather than slogans.