AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 4 of 7

KYT & Blockchain Transaction Monitoring Requirements

Know Your Transaction Standards for Digital Asset Firms
AML & Sanctions Practices in the Digital Asset Industry

Transaction Monitoring (KYT - "Know Your Transaction") and Blockchain Analytics

KYT, or Know Your Transaction, refers to the continuous monitoring of transactions to detect suspicious or illicit activity. In the crypto context, this takes on a specialized meaning: because blockchains are transparent, blockchain analytics tools can be used to trace funds and identify whether crypto addresses involved in transactions are linked to criminal enterprises, sanctioned entities, darknet markets, fraud scams, ransomware, or other red flags. Effective KYT means an exchange or financial institution doesn't just KYC the customer at onboarding - it also watches how that customer's crypto funds move, to spot any indication of money laundering or other prohibited behavior. Implementation of KYT includes automated transaction monitoring systems, blockchain analysis software, case management for investigations, and reporting of suspicious activities to authorities.

Here's how this is done across different setups:

Transaction Monitoring in Centralized Exchanges (CEX)

Centralized exchanges typically hold customers' crypto in deposit addresses or wallets under the exchange's control. They can therefore monitor all inflows and outflows to those wallets, as well as platform trading activity. Modern exchanges integrate real-time blockchain analytics solutions - such as Chainalysis KYT, TRM Labs, or Elliptic - to automatically screen cryptocurrency transactions against known risk indicators.
For example, if a user of an exchange attempts to deposit coins originating from a flagged source (e.g., a hack or a darknet marketplace), the analytics tool will raise an alert. Chainalysis's KYT software, for instance, provides automated alerts whenever funds touch wallets associated with sanctions, darknet markets, ransomware, mixers, or other high-risk categories.

The tool maintains an attribution database that maps thousands of addresses and entities, enabling it to label transactions (e.g., “this deposit came from a wallet that is 2 hops away from a known scam address”). Exchanges configure risk rules within these systems - for instance, flag any transaction above $X from a privacy mixer service, or any interaction with an address that has >10% of its funds from illicit sources. If a rule is triggered, the system can either notify compliance staff to review or even automatically pause the transaction for investigation.

On the fiat side (since many exchanges also handle fiat on-ramps), exchanges use conventional AML transaction-monitoring software to monitor fiat deposits/withdrawals for structuring (smurfing) or other unusual patterns, much like a bank would. But the distinctive element in crypto is on-chain KYT: monitoring crypto flows across addresses. Exchanges like Coinbase and Binance have large in-house compliance teams (sometimes ex-law enforcement analysts) who investigate alerts by using graph visualization tools (e.g. Chainalysis Reactor or TRM Investigator) to follow the trail of funds. They look for patterns such as structuring: e.g. multiple sub-$3k transfers to avoid the $3k Travel Rule threshold (which could indicate a user is trying to evade reporting).

Other red flags include sudden velocity changes (a typically low-volume user suddenly moving huge sums), or multiple users sending to the same unknown wallet (potentially a sign of a third-party off-platform funnel) - these scenarios are often built into rules or monitored via dashboards. Indeed, exchanges take a risk-based approach: not every alert means wrongdoing, but it prompts review. Many exchanges employ tiered responses - contacting the user for explanation, temporarily freezing funds, raising the KYC level, or ultimately off-boarding the user - depending on the severity of the suspicious activity. Regulatory expectations are that crypto businesses have transaction monitoring equivalent to other financial institutions. In practice, this means filing Suspicious Activity Reports (SARs) (or Suspicious Transaction Reports, STRs, outside the U.S.) to the government when a transaction or series of transactions looks like it may involve criminal funds or other AML violations. For example, in the U.S., if an exchange reasonably suspects money laundering - say, a user receives deposits from a known darknet source and immediately cashes out - it must file a SAR with FinCEN within 30 days.

High-volume exchanges file large numbers of SARs, similar to banks. Regulators expect exchanges to have automated systems once manual review becomes insufficient - trying to monitor thousands of daily transactions by hand would be impossible, which is why they rely on software. Additionally, Currency Transaction Reports (CTRs) are required in the U.S. for any cash transaction at or above $10,000 - in crypto context, this might apply to cash-to-crypto transactions (e.g., large cash deposits to an exchange’s bank account to buy crypto).

Another key piece is the Travel Rule: in FATF member countries (including the U.S., EU, UK, Singapore, etc.), exchanges must comply with the Travel Rule for qualifying transfers. This means that when a customer of Exchange A sends crypto above a certain threshold (commonly $/EUR 1,000) to another exchange (Exchange B), Exchange A must collect and transmit the originator and beneficiary information (name, account details, etc.) to Exchange B alongside the blockchain transfer. As of 2024, about 65 of 98 surveyed jurisdictions had Travel Rule laws either implemented or in progress, and the EU's new rules removed the minimum threshold, requiring Travel Rule data for all crypto transfers between CASPs. In practical terms, exchanges have adopted tech solutions (e.g. Notabene, TRISA, OpenVASP, Sygna) to securely exchange this information. For instance, when a user on Coinbase (U.S.) wants to send 5 BTC to an address that Coinbase determines belongs to Binance (based on either address registries or user declarations), Coinbase will send Binance the required identifying information out of band. This is a quickly evolving area - by 2025 many large exchanges have integrated Travel Rule APIs, but industry-wide interoperability is still being worked out, and not all countries enforce it strongly yet. Nonetheless, regulators consider Travel Rule compliance a clear expectation for centralized VASPs.

Beyond blockchain analytics, exchanges also monitor off-chain user behavior: login patterns, device or IP changes, and fiat transaction behaviors for fraud or sanctions risk. Companies like Sardine offer AI-based risk scoring that combines customer profile, device, and historical patterns to flag unusual activity (bridging fraud prevention and AML). Such tools might catch, for example, a user who suddenly logs in from a high-risk country or tries rapid back-to-back withdrawals - indicating account compromise or mule activity. In summary, CEXs employ a multilayered KYT approach: blockchain surveillance for on-chain risks, rule-based monitoring of transactions (crypto and fiat), and case management workflows that escalate alerts to human investigators and ultimately to regulatory reports.

Transaction Monitoring in DeFi

True decentralized platforms do not have built-in transaction monitoring or reporting, since transactions occur directly on the blockchain without an intermediary to oversee them. However, this does not mean DeFi transactions go unwatched - rather, monitoring is carried out externally by analytics firms, compliance teams of other entities, and law enforcement. For instance, even though Uniswap itself isn't filing SARs, analytics companies (Chainalysis, Elliptic, TRM) and government agencies are actively tracing flows through DeFi protocols to identify patterns of illicit activity (such as hacker funds being swapped on DEXs). DeFi projects with a company presence may choose to implement some preventative measures: as noted, interfaces can block known bad addresses from interacting with their dApps. This is a form of rudimentary KYT - essentially preventing certain transactions altogether if they involve blacklisted addresses.

One example is how certain DeFi front ends integrated TRM Labs' API to refuse service to wallet addresses associated with North Korea's Lazarus Group after high-profile hacks. Another example is automatic blacklisting by stablecoin issuers: Circle (USDC) and Tether (USDT) have, at the protocol level, frozen addresses on the Ethereum blockchain when directed by authorities (effectively censoring transactions of sanctioned or illicit actors). These actions intersect with sanctions compliance but also serve AML goals. There are also emerging on-chain analytics protocols that aim to provide risk scores for addresses that anyone can query (for example, Blocktrace and others have explored decentralized risk-scoring oracles).

Yet, no DeFi protocol today performs the kind of ongoing, individualized transaction surveillance that regulated intermediaries do. If a money launderer is mixing funds through a series of DeFi swaps, the protocol isn't filing an alert - instead, it might be an exchange that those funds eventually hit, which files the SAR, or law enforcement monitoring the blockchain and then issuing subpoenas to any touchpoints (like centralized bridges or off-ramps). Regulators recognize this gap and, in various reports (such as the U.S. Treasury's 2023 DeFi Risk Assessment), have signaled that if DeFi platforms are truly decentralized with no entity in charge, they fall outside current AML regulations - a loophole being misused by illicit actors. Therefore, guidance is evolving to expand the definition of a VASP to include persons involved in DeFi operations, so that someone can be held responsible for KYT/AML.

The challenge remains significant: enforcing the Travel Rule or implementing transaction monitoring for peer-to-peer wallet transactions in DeFi is technically and legally complex. As of 2025, the practical industry approach is that compliance largely happens at the on/off-ramps: when funds move from DeFi into a centralized exchange or fiat, that's where traceability and monitoring lead to action. DeFi protocols themselves are starting to consider integrating compliance features optionally (e.g., Uniswap's announcement in 2023 of an optional compliance tool for enterprises), but wholesale adoption of KYT in DeFi is still nascent.

Transaction Monitoring by Other Crypto Firms

Many other crypto businesses implement KYT in ways analogous to exchanges. Crypto payment processors will screen the blockchain addresses from which they receive funds or to which they send funds on behalf of merchants. Custodians and crypto banks use analytics to ensure assets they custody aren't tainted. Even venture funds and OTC brokers often use tools to conduct due diligence on the sources of crypto they handle (for reputational reasons). Mining pools have started to use transaction screening: some U.S.-based Bitcoin mining pools comply with OFAC guidance by not processing transactions from sanctioned addresses - this is a form of KYT at the protocol level (though controversial in the community).

Another key development is collaboration among organizations such as Crypto Defiance and the Crypto Market Integrity Coalition, where exchanges and analytics firms share typologies of crypto-specific illicit behavior, refining the red flags for this industry.
By 2024, it's become standard for any serious crypto business to use one of the major blockchain analytics providers or an equivalent in-house system. In fact, blockchain tracing capability is often cited to exceed traditional banking in some respects, because it allows following the provenance of funds in an immutable ledger across multiple hops and even across multiple VASPs. Regulators encourage crypto firms to leverage that transparency to "know their transactions" deeply - for instance, OFAC's guidance suggests that crypto firms integrate all available data, including blockchain data and user IP addresses, to spot sanctions/AML risks.

Blockchain Analytics and Transaction Monitoring: Tools in Use

The leading analytics firms - Chainalysis, TRM Labs, and Elliptic - are widely used by industry and government. Chainalysis KYT is often described as the industry standard, offering real-time monitoring over 10,000+ digital assets with risk alerts for interactions with illicit entities. It allows compliance teams to set custom rules and has investigation tools (Reactor) for deep dives. Elliptic focuses on high-precision wallet screening and entity-level risk scoring, boasting a large data set of attributed actors and low false-positive rates. TRM Labs differentiates with AI-driven risk detection, claiming to catch novel patterns before they're formally flagged (useful for emerging threats).

TRM also has a built-in case management and a Travel Rule solution to facilitate counterparty information exchange. These analytics tools are typically integrated via API into exchanges' internal systems - for example, when a user requests a crypto withdrawal, the system automatically pings the analytics API to score the destination address; if high risk, the withdrawal is held for review. Likewise, incoming deposits are screened in real-time and can be auto quarantined if from blacklisted addresses. Exchanges often use multiple analytics providers to achieve broader coverage (one may be stronger at tracing certain assets or new blockchains than another). Other notable tools: CipherTrace (owned by Mastercard), which provides transaction monitoring and a Travel Rule solution (Traveler), Merkle Science (focus on predictive risk scoring), Blockchain Intelligence Group (QLUE), Scorechain, and smaller startups specializing in DeFi analytics (like Blockspan, Nansen for tracing smart contract interactions, though Nansen is more for research than compliance). Notably, even government agencies use these same tools - e.g., U.S. ICE and IRS have contracts with Chainalysis and TRM - so when an exchange uses them, it aligns their view with what regulators might see.

Travel Rule Solutions

Complying with the Travel Rule has spawned an entire sub-industry. Notabene provides an end-to-end Travel Rule platform that enables VASPs to securely route compliance data to one another. TRISA (Travel Rule Information Sharing Alliance) is an open-source consortium solution, and OpenVASP (originating in Switzerland) provides a decentralized protocol using ENS domains for VASP identity. Sygna Bridge (by CoolBitX) is popular in Asia for Travel Rule messaging. The EU's adoption of a unified approach (through the Transfer of Funds Regulation update) has pushed many European CASPs to sign up for interoperability pilots among these providers. By 2025, many exchanges have either built or adopted a Travel Rule compliance service but connecting them all is ongoing. We also see chain-specific solutions - e.g., for Bitcoin Lightning or certain privacy coins, proposals for how to handle Travel Rule data (though privacy coins pose a dilemma; some exchanges just delist those assets to avoid inability to comply with Travel Rule).

KYT Comparative Summary

The table below summarizes transaction monitoring and KYT controls across CEX, DeFi, and other businesses:

Dimension	Centralized Exchanges / Custodians	Decentralized Platforms (DeFi)
On-chain analytics	Extensive use of blockchain analytics tools (Chainalysis, TRM, Elliptic) to flag transactions involving illicit or high-risk wallet addresses. Automated alerts for funds touching mixers, darknet markets, sanctioned addresses, etc. Compliance teams investigate alerts using on-chain tracing tools.	No built-in analytics; protocol treats all transactions equally. Any screening is external. Some front-ends or token issuers voluntarily block or flag known illicit addresses, but users can often interact directly with the smart contracts to bypass front-ends. DeFi relies on external observers (analytics firms, law enforcement) to monitor flows on the public ledger.
Off-chain monitoring	Monitors customer behavior on the platform: trade patterns, deposit/ withdrawal sizes vs profile, rapid movements, structuring attempts (e.g. multiple sub-threshold transfers). Fiat transactions also monitored (integration with bank AML systems). Suspicious patterns trigger case review and possible account freeze or enhanced due diligence.	Not applicable at protocol level (no concept of customer profiles or off-chain behavior in pure DeFi). Any off-chain monitoring would be by a user's wallet app or an interface plugin, but this is uncommon. DeFi transactions are pseudonymous and algorithm-driven, so traditional behavior monitoring isn't present.

Dimension	Centralized Exchanges / Custodians	Decentralized Platforms (DeFi)
Regulatory reporting	Required to file SAR/STRs for any transaction deemed suspicious (e.g. signs of money laundering, terrorism financing). Large exchanges file thousands of SARs per year to FinCEN or local FIUs. Also file currency reports for cash transactions at or above $10k. Must implement FATF Travel Rule: collect and transmit sender/recipient data for crypto transfers above designated thresholds. Non-compliance (e.g. failing to report suspicious activity) can lead to significant fines.	DeFi protocols are not currently regulated as reporting entities, so they typically do not file SARs or collect Travel Rule information. (In fact, there is usually no mechanism to do so.) However, users or intermediaries who touch DeFi (like a regulated exchange that sees a customer sending funds to a DeFi protocol) do have to report suspicious flows involving DeFi. As regulators consider new rules, it's possible certain persons (like DAO members or front-end operators) may be tasked with reporting in the future, but this is not yet in force.
Other Crypto Businesses	If classified as a VASP or financial institution, they have the same reporting duties as exchanges. Many wallet and payment service providers in the U.S. and EU are MSBs and do file SARs. For example, a crypto ATM operator must file SARs if they notice suspicious structuring by a user. Travel Rule obligations also apply to many non-exchange VASPs (custodians, brokers), and they use solutions to comply (some partner with Travel Rule networks to handle data exchange).	Similar story: any entity with regulated status must implement equivalent KYT. Non-custodial services are starting to incorporate KYT: for instance, a wallet app could warn a user sending to a scam address. With Travel Rule, any entity defined as a VASP must comply when transacting with another VASP. Many have joined Travel Rule networks (Notabene, TRISA, etc.) or use in-house solutions to transmit required data.