AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 6 of 7

AML Program Governance, Controls & Operating Models

Building & Running Effective AML Programs in Digital Asset Firms
AML & Sanctions Practices in the Digital Asset Industry

Digital Assets AML Programs and Controls

Beyond KYC/KYB and transaction monitoring, crypto institutions are expected to maintain an overall AML/CFT compliance program that mirrors the programs in traditional finance. This includes internal governance, written policies and procedures, training, independent audits, and record-keeping - all tailored to the crypto business model. Both U.S. regulations and FATF guidance emphasize a risk-based approach: firms should assess their specific risks (e.g., retail exchange vs. institutional custodian vs. peer-to-peer platform) and implement controls commensurate with those risks. Below are key elements of AML programs in the digital asset industry and how they compare across entity types:

Centralized Exchanges and Regulated VASPs

A CEX's AML program is often quite formal and robust by 2024, especially for those operating in multiple jurisdictions. Typical components include:
Compliance Officer and Team

Appointment of a Chief Compliance Officer (CCO) or BSA Officer who is responsible for day-to-day compliance and liaising with regulators. Large exchanges have entire departments with dozens or hundreds of staff for KYC onboarding, transaction monitoring, investigations, and regulatory reporting.

Policies and Procedures

Written AML/CFT compliance manuals that outline how KYC, KYB, KYT, sanctions, and reporting are handled. These are regularly updated to reflect new laws (for instance, if a country introduces a stricter travel rule threshold, the procedures are amended). Regulators (such as NYDFS in New York or FINMA in Switzerland) often require the submission or inspection of these policies.

Risk Assessment

Exchanges conduct enterprise risk assessments to identify inherent risks (customer profile, geographic exposure, product or service offerings such as privacy coins or derivatives, etc.) and to evaluate the effectiveness of their controls. For example, an exchange serving high-risk jurisdictions or offering anonymity-enhanced cryptocurrencies must document how it mitigates those risks (perhaps by not serving certain areas or delisting privacy coins).

Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

Procedures for standard CDD (basic KYC) and triggers for EDD. EDD might involve obtaining information on the source of funds/wealth for a customer who is high-value or high-risk (e.g. a politically exposed person or someone from a country with weak AML laws). Some exchanges require a source-of-funds declaration and evidence for large fiat deposits or withdrawals, aligning with banking practices.

Ongoing Monitoring and Screening

As covered, continuous monitoring of transactions and periodic rescreening of customers. Also, keeping customer information up to date (exchanges may periodically prompt users to refresh their KYC details or to provide updated ID if the old one has expired).

Suspicious Activity Reporting

Clear internal processes for escalating potential suspicious activity, decision-making on filing a SAR, and timely filing. In the U.S., SARs must be filed within 30 days of detecting facts that form the basis of suspicion. Employees are trained to flag unusual behavior to the compliance team. Some exchanges have automated SAR drafting tools integrated into their case management systems, though human review is always required.

Regulatory Reporting

Besides SARs/STRs and CTRs, exchanges comply with other reporting like annual or quarterly reports to regulators if required, and respond to law enforcement requests (subpoenas, etc.). For instance, FinCEN-registered MSBs must renew their registration every 2 years and keep certain records (such as records of transmittals at or above $3k, per FinCEN rules). In the EU, CASPs will report to national authorities and soon to the new EU AML Authority (AMLA) once established.

Independent Audit

AML programs must be tested by independent auditors or compliance consultants periodically (e.g., annually) - this is required under U.S. regulations for MSBs and under

many jurisdictions' laws. Crypto companies often hire firms to conduct a compliance program audit, testing whether alerts are handled properly, whether KYC files are complete, etc., and producing a report with findings to improve.

Training

Staff, especially those in customer-facing roles or compliance, receive regular AML training. This covers recognizing red flags, new typologies (such as DeFi risks and NFT money laundering), and company procedures. Many exchanges hold annual training sessions and require new hires to complete AML training upon joining.
Overall, a well-run exchange's AML program in 2025 looks much like that of a mid-size bank, albeit incorporating crypto-specific tools and addressing crypto-specific risks.

Regulators have explicitly said there's no "one size fits all," but they expect exchanges to document and follow strong controls appropriate to their risk profile. The consequences of inadequate programs have been severe: for example, Binance's massive 2023 settlement (with DOJ, OFAC, FinCEN, and CFTC) revealed that the exchange had willfully violated AML laws by having porous controls, especially in its early years, allowing customers in sanctioned countries and criminals to use the platform. The $4.3B penalty and requirement for an independent monitor underscore that regulators will impose costly consequences if a crypto platform operates without an effective AML program. Likewise, Coinbase's $100M settlement with New York in 2023 was specifically for failures in its AML compliance - it grew too fast for its compliance systems, leading to backlogs in KYC reviews and monitoring alerts, which regulators viewed as unsafe. These cases have effectively rewritten the playbook by demonstrating that investment in compliance is far cheaper than the fallout of enforcement.

AML Controls in DeFi

Decentralized platforms, having no centralized compliance team, do not have formal AML programs. The protocol typically provides no compliance officer, no SAR filing, and no KYC. Some argue that the code itself is "the compliance" (e.g., all transactions are transparent on-chain, and smart contracts can't discriminate), but from a regulator's perspective, this is not sufficient to meet AML obligations.

At present, AML for DeFi is handled indirectly: the entities surrounding DeFi (centralized exchanges providing fiat ramps, or even users themselves who are regulated entities) pick up the slack. For instance, when stolen crypto from a DeFi hack is laundered through multiple DEX trades and then deposited into a regulated exchange, the exchange's AML program will detect anomalies and potentially freeze funds in cooperation with law enforcement.

Another facet is community-driven compliance: some DeFi protocols are discussing implementing DAO proposals to block certain illicit addresses at the smart contract level (this has been controversial, as it clashes with ideals of neutrality and censorship-resistance). The regulatory expectation for DeFi is still being formed. FATF has made clear that if there is any person with influence (e.g., a founder who can upgrade a contract or a multi-sig that controls treasury), authorities can impose AML obligations on them as VASPs. But truly autonomous DeFi with no legal entity remains a gap - for now, regulators are focusing on guidance and warnings.

The U.S. Treasury's 2023 report on DeFi illicit finance suggested exploring compliance by design (building AML tools into new DeFi projects) and hinted at future rulemaking to address non-compliant DeFi. Europe's MiCA framework largely sidestepped DeFi, but a report/review is expected in 2024-25 which could lead to new EU rules. In short, AML programs as traditionally defined do not exist in DeFi protocols in 2024, and this is an area of ambiguous, evolving guidance. We may eventually see hybrid models (e.g. semi-decentralized platforms registering as VASPs and doing KYC/AML on users while still leveraging smart contracts), but the fully decentralized ones are currently operating in a regulatory grey zone.

AML in Other Blockchain-Native Firms

Many other crypto firms actually do have formal AML programs, especially if they have a corporate structure. For example, crypto custodians, crypto broker-dealers, crypto investment funds, and money transmitters using crypto all must have internal controls similar to those of exchanges.

A notable subset is financial institutions adopting crypto: for instance, banks that offer crypto custody or trading incorporate those activities into their existing AML programs (subject to bank regulator exams).

Another example: money service businesses like MoneyGram and Western Union have started integrating crypto transfers; they extend their AML controls (which are very mature) to those services. Stablecoin issuers (if regulated under trust charters or as electronic money in some regimes) maintain compliance teams to monitor transactions (Circle, for example, has compliance personnel and cooperates with authorities to track illicit flows of USDC).

Publicly listed mining companies implement compliance measures to ensure mined coins aren't sent to bad actors. And web3 startups aiming to work with banks find that they must build compliance programs early to gain banking partners or licenses. For instance, Ripple (the company) was fined by FinCEN back in 2015 for AML lapses and, since then, has operated a compliance program for its cross-border payment network.

Similarly, BitGo, a wallet provider, settled with OFAC in 2020 for $98K over sanctions violations and has since tightened its controls (such as IP address blocking and KYC requirements for some services). The trend from 2024 onward is that any crypto service that wants to be seen as reputable will voluntarily adhere to AML best practices even if not explicitly required by law, because it facilitates partnerships and pre-empts future regulation.

We also see crypto firms hiring former regulators and experienced compliance officers to bolster their programs, recognizing that compliance is a competitive advantage (it builds trust with users and regulators).

In summary, centralized and institutional crypto firms have converged on applying traditional AML program structures, while DeFi and truly decentralized ecosystems remain an outlier which regulators are scrutinizing.

Fraud and Risk Platforms Enabling AML

In addition to AML-focused tools, crypto companies use fraud prevention tools, which often complement compliance. Sardine is one such platform known in the crypto on-ramp space; it uses AI to analyze customer behavior, device, phone, email, and other signals to predict fraud and money mule activity. While its primary aim is fraud (stopping stolen card use, account takeovers, etc.), this also supports AML by intercepting accounts that could be involved in illicit activity before it happens. Other platforms like Forter, Riskified, Feedzai, Socure are used by some crypto-financial services to handle identity verification with fraud scoring (e.g., Socure provides KYC plus synthetic identity detection). Chainalysis even partners with some KYC firms (e.g., TRM partnered with Sumsub in 2023) to offer integrated solutions combining on-chain and off-chain risk data.

Technological Solutions and Standardization

Another evolving area is the development of standards and protocols to improve compliance efficiency. For instance, messaging standards for Travel Rule (like the InterVASP IVMS101 data model) are now established, but ensuring all VASPs adhere is ongoing. API standards for blockchain analytics or for integrating identity verification are being discussed in industry groups. The goal is to reduce ambiguity by having common frameworks - if every VASP uses interoperable protocols for sharing KYC/KYB data or for Travel Rule, it's easier to comply. In 2024, the Travel Rule still faced challenges of interoperability, which is gradually improving through alliances and tech bridges (like Notabene's network connecting multiple Travel Rule protocols). There's also exploration of how CBDCs (central bank digital currencies) might incorporate automated compliance features, which could, in turn, indirectly set expectations for crypto. This is more speculative, but worth noting that if governments design digital currencies with built-in monitoring, they may expect similar transparency from crypto.

Clear vs. Ambiguous Guidance: A Practical Recap

In general, guidance is clearest for centralized, intermediated activities - e.g., custodial exchanges must do KYC, KYB, KYT, etc. and regulators have published manuals and fines that make expectations plain. Where guidance is ambiguous or developing, it concerns activities that are novel to crypto's decentralized paradigm or tangential to financial services. DeFi is the prime example, as repeated above. Others are certain applications of crypto like DAOs (if a DAO provides financial services, who is responsible for AML? Currently unclear - by 2026 we may have legal precedents or new rules addressing this). We also see evolving guidance in cybercrime-related AML, such as how to treat seizure of stolen crypto, how exchanges should handle ransomware payments (e.g., some countries might mandate blocking ransom payments, others require reporting them - not uniformly codified yet).

The industry is closely watching regulators' publications for more clarity. In late 2025, for example, TRM Labs' Global Crypto Policy Review noted that over 30 jurisdictions introduced or refined crypto-compliance regulations that year alone, signaling rapid change. Firms must stay agile and often seek legal counsel to interpret new rules. Collaboration between industry and regulators is increasing to clarify grey areas - through consultation papers, regulatory sandboxes, and industry associations (such as Global Digital Finance's working groups) that issue best-practice guidance where the law is silent.

AML Program Comparative Summary

The table below highlights differences in overall AML program implementation across entity types:

AML Program Element	Centralized / Regulated Entities	Decentralized / Unregulated Protocols
Governance & Staffing	Appoint a dedicated compliance officer (e.g., BSA/MLRO) and team. Formal governance with board oversight in larger firms. Regular audits and regulator inspections.	No formal governance for compliance. Code is open-source and managed by the community or developers with no compliance department. (Some DeFi projects have informal risk working groups, but nothing equivalent to a compliance office.)
Policies & Procedures	Detailed written AML/CFT policy, customer acceptance policy, sanctions policy, etc., tailored to crypto risks (e.g., addressing peer-to-peer transfers, use of mixers). Updated frequently to reflect new laws or typologies.	None at the protocol level. (Individual users or liquidity providers aren't bound by any AML policy beyond general law.) Any "policy" exists only if developers publish compliance guidelines, which is rare.

AML Program Element	Centralized / Regulated Entities	Decentralized / Unregulated Protocols
Training & Culture	Regular AML training for staff; compliance culture increasingly prioritized in big exchanges (especially post-enforcement actions). Some exchanges integrate automated compliance checks into product development (culture of "compliance by design").	No staff means no formal training. The user community is generally not educated on AML obligations (except perhaps caution about obvious scams). Compliance culture is not a concept in autonomous protocols - the culture instead emphasizes privacy and decentralization, sometimes at odds with AML norms.
Regulator Engagement	Active engagement: licensed crypto businesses must undergo examinations by regulators (e.g., FinCEN or state regulators in the US, FINTRAC in Canada, FCA in the UK). They respond to findings, improve programs, and sometimes participate in industry regulatory committees. Larger firms lobby and provide feedback on new regulations.	Typically, there is no direct regulator interaction since there is no entity to supervise. However, developers/founders may be called before legislatures or hearings (as happened with certain DeFi projects) but they aren't "examined" in an AML sense. Some DeFi projects collaborate proactively with law enforcement on specific investigations (tracing stolen funds), but this is ad hoc.
Other Entities (Wallets, Fintechs, etc.)	Those with licenses (money transmitters, etc.) get examined. Others may proactively obtain third-party certifications (e.g., SOC reports that include compliance controls) to assure partners. Many fintechs working in crypto build open lines of communication with regulators to ensure they won't be caught off guard by compliance expectations.	Companies in less-regulated sectors (say, an NFT marketplace in 2024) may have no formal AML program - but this is changing as jurisdictions plan to include such sectors in AML laws (e.g. EU considering NFTs, and FATF advising risk-based AML measures for NFT platforms where relevant). The trajectory is that any crypto-related business type that becomes significant will be folded into the AML regulatory scope, so many are preemptively establishing compliance programs ahead of mandates.

Dimension	Centralized Exchanges / Custodians	Decentralized Platforms (DeFi)
Other Crypto Businesses	Same expectations as for exchanges. Any business with a U.S./EU nexus must not transact with sanctioned parties. Wallet providers and others learned this through enforcement (e.g. OFAC fines to BitGo in 2020, BitPay in 2021, and Exodus/ShapeShift in 2025 for sanctions violations). These firms now have sanctions compliance programs: they collect at least IP or geolocation data to block access to embargoed jurisdictions, and they screen any identifiable customer data. Services like stablecoin issuers can freeze tokens for sanctioned individuals (as happened with USDT and USDC addresses). Even miners have, informally, complied (some mining pools refuse transactions to OFAC-sanctioned addresses to avoid facilitating prohibited transactions).	Consistent sanctions gap in purely decentralized operations. Regulators are studying whether developers or DAO participants could be liable for facilitating sanctions evasion, but practical enforcement in DeFi remains limited. The few exceptions are truly decentralized operations, which remain a headache for sanctions enforcement and likely targets for future regulation or technical solutions.