AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 2 of 7

KYC Controls Across Centralized, Decentralized & Hybrid Models

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

Know Your Customer (KYC) Practices in Crypto

KYC refers to verifying the identity of individual customers during onboarding and periodically thereafter to establish that they are who they claim to be and to assess associated risks. It is a cornerstone of compliance for any regulated financial service, including crypto exchanges. In practice, KYC entails collecting personal identifying information and documents, verifying their authenticity, and screening the individual against watchlists (sanctions lists, politically exposed persons lists, etc.).

Below, we detail current KYC practices:

KYC in Centralized Exchanges (CEX)

Nearly all major centralized crypto exchanges and custodial platforms require customers to complete identity verification before granting full access. This typically includes providing a government-issued photo ID (passport, driver's license, or national ID), proof of address (utility bill or bank statement), and sometimes a selfie or live video for facial biometric matching. For example, exchanges like Binance, Coinbase, and Kraken require KYC verification for users to deposit, trade, or withdraw amounts beyond minimum limits. There is no one global KYC standard — requirements vary by jurisdiction and risk appetite — but most mainstream exchanges collect far more than just a name and email, especially if users will transact significant volumes. Some exchanges employ a tiered KYC system: basic tiers (with email or phone verification) allow only small trades, whereas higher tiers (requiring full ID documents and sometimes supplemental due diligence) unlock larger transaction limits.

In the U.S. and EU, regulatory expectation is that any customer who trades or transfers above trivial amounts must be identity-verified as part of Customer Due Diligence. Exchanges implement KYC by integrating digital identity verification solutions — e.g.

Jumio, Onfido, Trulioo, Sumsub, Veriff — which use document scanning, optical character recognition, and biometric checks to validate IDs and match selfies to IDs in real time. Biometric "liveness" tests (to ensure the person is physically present and not using a spoof) are also increasingly used. After collecting KYC info, exchanges perform name screening: comparing the customer's name (and sometimes other identifiers, such as date of birth) against sanctions lists (OFAC's SDN list, UN sanctions, EU/UK sanctions) and against databases of politically exposed persons (PEPs) or adverse media. Specialist providers like Refinitiv World-Check or Thomson Reuters are often used to automatically flag if a new customer is a sanctioned individual or high-risk PEP. If a positive match or other red flag appears, the exchange will typically pause onboarding that customer pending further due diligence or reject the customer. Ongoing monitoring is also part of KYC: even after initial verification, exchanges periodically rescreen their user base against updated sanctions/PEP lists and may require KYC refresh (e.g., update of ID documents) for long-standing accounts or when a user's activity changes risk profile.

The practical execution of KYC at CEXs is highly digitized — new users often go through an app or website flow to upload documents and selfies, with automated systems (sometimes AI-powered) verifying information within minutes. Compliance teams then handle exceptions or edge cases manually (e.g., if document images are unclear or if fraud is suspected). KYC data is retained for the required period (5+ years in many jurisdictions) and is subject to strict access controls due to privacy regulations such as GDPR.

From a regulatory standpoint, CEXs' KYC controls are expected to follow a risk-based approach: collect sufficient information to verify identity and assess risk, while allowing some flexibility for low-risk, low-volume users. FATF and national regulators encourage financial inclusion, meaning exchanges can offer flexible tiered KYC to avoid excluding unbanked customers — but ultimately, any customer transacting beyond very low thresholds must be fully verified. Failure to implement adequate KYC has led to enforcement actions. For instance, U.K. officials fined Coinbase's UK entity £3.5 million in 2020 for onboarding 13,000+ "high-risk" users without proper enhanced KYC checks. In 2024 alone, KYC deficiencies accounted for about one-third of all compliance penalties in the crypto sector (around $1.25 billion in fines), reflecting regulators' focus on customer identification controls.

KYC in Decentralized Finance (DeFi) Platforms

In contrast to CEXs, most DeFi platforms (DEXs, lending protocols, etc.) do not perform KYC on users in the traditional sense. Decentralized exchanges like Uniswap or PancakeSwap are non-custodial and allow wallet-to-wallet trading via smart contracts without any identity checks. Users interact via pseudonymous blockchain addresses; there is no centralized intermediary to request IDs or verify identities, so KYC is essentially

absent at the protocol level. This anonymity is philosophically aligned with DeFi's origins, but creates a compliance gap: no one is verifying that DeFi users are not criminals or sanctioned persons. Regulators have voiced concern that criminals can exploit non-KYC platforms.

In fact, the anonymity of DeFi is cited as a major risk, and global AML standard-setters are seeking solutions. As of 2025, KYC in DeFi remains largely voluntary or external. For example, certain front-end websites (the interfaces that users use to access DeFi protocols) have started geo-blocking IP addresses from sanctioned jurisdictions or blocking wallet addresses associated with sanctions or hacks, using blockchain analytics data. In mid-2022, Uniswap's web interface began blocking addresses flagged by TRM Labs as linked to illicit activity, and MetaMask/Infura have blocked users from countries under U.S. sanctions. However, these measures are not foolproof (users can switch wallets or use VPNs), and they stop short of true KYC since they do not reveal the user's identity. No major DeFi protocol currently requires users to submit IDs before using the smart contracts — doing so would undermine the open-access nature of decentralized services.

That said, we are seeing the rise of "permissioned DeFi" for institutions: for example, Aave Arc is a liquidity pool restricted to whitelisted institutional participants who have undergone KYC/KYB by a third-party facilitator. Similarly, some projects issue KYC-NFT tokens or verifiable credentials that attest that a user has been KYC-verified by a provider, which could allow DeFi smart contracts to verify credentials without handling the user's personal data. These are experimental and not widely adopted yet. Regulatory expectations for DeFi KYC are evolving: FATF guidance (2021) suggests that if a "DeFi" arrangement is not fully decentralized — i.e., if there are persons with control or sufficient influence (developers, owners of admin keys, etc.) — those persons may be deemed VASPs and obligated to perform AML/KYC. Enforcement is nascent; one notable action was OFAC's 2022 sanctions against the Tornado Cash smart contract mixer, effectively blacklisting a DeFi tool for illicit use. This indicates that authorities are willing to act at the protocol level for egregious cases, even though routine user-by-user KYC in DeFi is not yet in place.

In summary, KYC on true decentralized platforms is currently minimal to non-existent, which regulators flag as a gap but have not fully resolved as of 2025. Users can often access DeFi services with only a crypto wallet and no identity verification, an area with ambiguous, evolving guidance.

KYC in Other Blockchain-Native Financial Institutions

Beyond exchanges and DeFi, there are other crypto financial services — e.g., custodial wallet providers, crypto payment processors, Bitcoin ATMs, stablecoin issuers, crypto lending/borrowing platforms, and crypto-based fintechs — each with their own approach to KYC. Generally, if a service involves custody of assets or conversion between crypto and fiat, it is likely subject to the same KYC requirements as exchanges.

For instance, a custodial wallet or brokerage (such as Crypto.com or BlockFi when it was operational) will implement standard KYC on its users, since it holds customer funds and facilitates transfers. Stablecoin issuers like Circle (USDC) and Paxos (USDP) perform KYC for customers who directly mint or redeem stablecoins (treating them similarly to bank account holders), even though secondary-market trading of stablecoins between unknown parties can occur on-chain.

Crypto ATMs (BTMs) in many countries require users to scan an ID or at least a phone number if transacting above certain limits, pursuant to MSB regulations. Payment processors and crypto remittance services (e.g., BitPay or Ripple's On-Demand Liquidity partners) must KYC their client businesses and sometimes end users, depending on their role.

An emerging area is Web3 gaming or NFT marketplaces — currently, most NFT platforms do not do KYC for buyers/sellers of digital collectibles, but if those assets are deemed financial (or in jurisdictions like the EU, which plan to cover NFTs under AML rules if used for payment), KYC obligations may arise. One notable enforcement action illustrating KYC expectations, even for "tech" providers, was OFAC's action against Exodus Movement, Inc. in 2025. Exodus provides non-custodial crypto wallet software (users hold their own keys) and historically has not collected user information. However, OFAC fined Exodus ~$3.1 million for providing services (support and software updates) to users in Iran, noting that merely having a Terms of Service banning sanctioned users was insufficient — Exodus had no effective way to enforce location or identity restrictions, and even had staff advising Iranian users on VPNs.

As part of the settlement, Exodus had to invest in sanctions compliance controls, effectively pushing a non-custodial actor to implement screening. This exemplifies a broader trend: even "blockchain-native" firms that historically didn't do KYC (because they only provided software or decentralized services) are coming under pressure to implement basic KYC/screening measures if they have any U.S. or EU nexus.
Overall, any business in the digital asset space that interfaces with customers in a meaningful way is moving toward KYC adoption, either due to direct regulation or through indirect pressure (banks and payment partners demand their crypto partners be KYC/AML compliant, or else they sever ties).

Identity Verification Technology: Tools in Use

To onboard individual customers at scale, crypto firms use eKYC vendors that can quickly verify IDs and detect forgeries. Jumio and Onfido are popular for document verification (scanning passports/IDs and matching selfies). Trulioo, Veriff, Sumsub, Persona, and Auth0 (Okta) are also commonly integrated into exchange signup flows. These providers offer SDKs that capture user ID images, run forensic checks (hologram detection, MRZ reading, etc.), and sometimes database checks (comparing against known identity theft info). They also perform biometric face matching. By using such tools, exchanges can approve the majority of new accounts in minutes, with only edge cases kicked to manual review. Biometric solutions (e.g. FaceTec) add liveness tests to ensure the person is real. Some exchanges have moved toward reusable digital identity — for example, leveraging government electronic ID systems (BankID in Nordic countries, Aadhaar in India, etc.) where available to verify users.

KYC Implementation Summary

The table below contrasts KYC practices across centralized exchanges, DeFi platforms, and other crypto financial service providers:

Aspect	Centralized Exchanges (CEX)	Decentralized Platforms (DeFi)
KYC Requirement	Legally mandated in most jurisdictions for customer onboarding. All users beyond trivial activity must be identity-verified.	Not required by protocol design; users transact pseudonymously without identity checks. Some front-ends impose geo-blocks or address blacklists, but do not collect IDs.
Data Collected	Email, full name, date of birth, government ID document, selfie, address proof, etc. Often tiered — basic info for low limits, full ID + proof-of-address for higher limits.	None collected on-chain. Users just connect wallets. Some DeFi interfaces may ask for nothing beyond wallet signature; a few might prompt country self-attestations.
Identity Verification	Automated eKYC solutions (Jumio, Onfido, etc.) verify document authenticity and match selfie to ID. Biometric liveness checks common. Manual review for exceptions. Name screened against sanctions/PEP lists via databases (Refinitiv, Comply Advantage).	No identity verification by protocols. Users remain anonymous, except for their blockchain address. Any screening is at network edges (e.g., a DEX front-end checking an address against a blacklist — which doesn't reveal identity, just blocks known illicit addresses).

Aspect	Centralized Exchanges (CEX)	Decentralized Platforms (DeFi)
Regulatory Status	Clearly required by AML laws for VASPs/MSBs. Regulators expect ongoing KYC updates and risk-based procedures (EDD for high-risk customers, etc.). Non-compliance leads to fines or loss of license.	Largely unregulated so far with respect to KYC, due to a lack of an identifiable operator. Regulators are exploring measures, e.g., the U.S. considering if DeFi front-ends can be treated as "brokers" in certain contexts, and the EU's MiCA calls for reports on DeFi by 2024. Guidance is evolving but not yet concrete.
Other Crypto Financial Services	If regulated or handling fiat (custodial wallets, payment processors, etc.), yes — they implement KYC similar to exchanges. Unregulated/non-custodial services typically do not collect KYC, though pressure is increasing to at least restrict sanctioned users.	Varies: Custodial services collect similar ID documents as exchanges. Crypto ATM users may input their phone and scan their ID above thresholds. Non-custodial software (e.g. decentralized wallet apps) collect no personal data. Enforcement cases (Exodus, ShapeShift) show authorities expect tech providers to avoid servicing prohibited persons.