From Brokerage to Blockchain

Developing an AML Framework for Crypto Trading Embedded in Brokerage Accounts

Executive Summary:

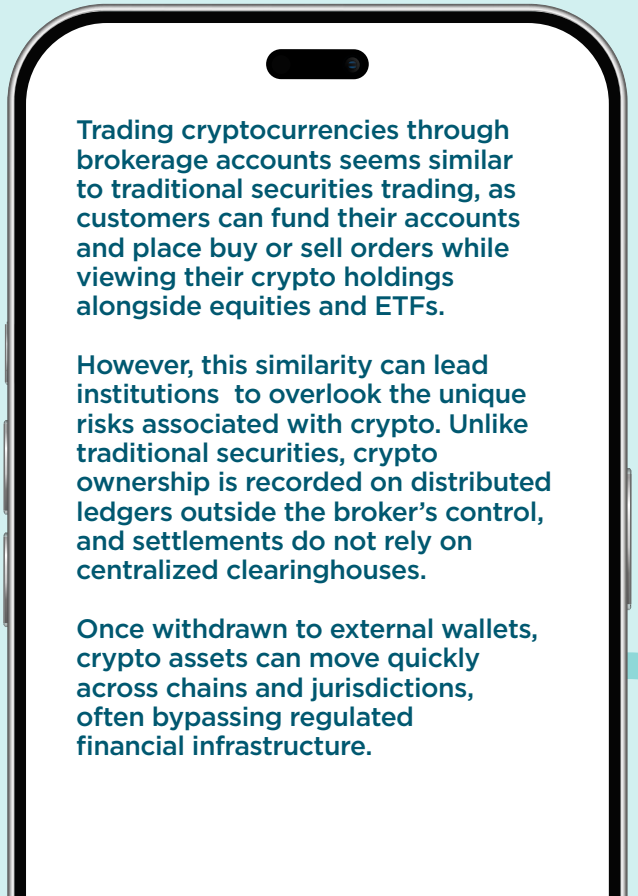
As cryptocurrencies gain mainstream acceptance, more banks, brokerage firms, and fintech companies are integrating crypto offerings into their services. U.S. regulators, including FinCEN and the SEC, have indicated that certain crypto asset activities can be permissible if conducted safely and in a well-governed manner.

However, incorporating crypto trading into brokerage platforms significantly shifts the anti-money laundering (AML) and sanctions risk profile. Crypto introduces structural challenges across customer onboarding, risk assessment, transaction monitoring, and sanctions compliance, driven by unknown counterparties and rapid asset mobility.

Institutions that apply traditional AML frameworks to cryptocurrencies without adjusting their approach often create control gaps, leading to monitoring blind spots and increased sanctions exposure, complicating regulatory compliance.

This white paper outlines an AML and sanctions framework for integrating crypto trading into brokerage accounts, highlighting why many banks' programs fail and emphasizing the importance of specialized crypto AML expertise for operational effectiveness and regulatory readiness.

The New Brokerage Reality: Why Crypto Is Different:



Trading cryptocurrencies through brokerage accounts seems similar to traditional securities trading, as customers can fund their accounts and place buy or sell orders while viewing their crypto holdings alongside equities and ETFs.

However, this similarity can lead institutions to overlook the unique risks associated with crypto. Unlike traditional securities, crypto ownership is recorded on distributed ledgers outside the broker's control, and settlements do not rely on centralized clearinghouses.

Once withdrawn to external wallets, crypto assets can move quickly across chains and jurisdictions, often bypassing regulated financial infrastructure.

Traditional brokerage AML programs are built around stable intermediaries, known counterparties, and predictable clearing and settlement flows. Surveillance focuses on market abuse, insider trading, and anomalous trading patterns within a closed ecosystem. While these risks remain relevant in crypto brokerage, they are accompanied by additional exposure to wallet-level interactions, layering through rapid asset swaps, cross-chain bridges, mixers, and indirect contact with illicit actors operating entirely outside regulated finance.

U.S. regulators emphasize that crypto trading institutions must adopt governance and control measures tailored to the risks involved, including anti-money laundering (AML) frameworks that address the relationship between crypto activities and fiat funding, custody, transfers, and external wallets.

AML Framework for Crypto Brokerage:

A credible Anti-Money Laundering (AML) framework for a crypto brokerage starts with a clear definition of scope, roles, and responsibilities across the entire crypto transaction lifecycle. Institutions must clearly specify whether they are acting solely as execution agents, facilitating fiat-to-crypto conversions, providing custody services, enabling withdrawals to external wallets, or supporting internal transfers between customers. Any ambiguity at this stage can undermine downstream controls and weaken regulatory compliance.

The key areas for the framework:

1 Customer Risk Management and Segmentation:

Crypto brokerage risk cannot be effectively managed using static KYC or traditional customer due diligence models alone. Customer risk varies significantly based on how crypto products are used, not simply on who the customer is. An effective framework segments customers dynamically based on crypto-specific behavior, including trading frequency, velocity of fiat-to-crypto conversion, use of external wallets, interaction with decentralized protocols, and patterns of asset movement. For example, long-term investors who hold assets in institutional custody have a fundamentally different risk profile compared to customers who frequently transfer assets through external wallets. Further, when assessing the risks of external wallets, institutions need to move beyond simple ownership classifications; they should implement confidence-based wallet attribution models that consider transaction history, behavioral consistency, and supporting evidence. This strategy enables more robust risk assessments by accounting for the uncertainties inherent in on-chain attribution.

2 Transaction Monitoring:

Crypto trading transaction monitoring should go beyond simply executing trades. It needs to track the entire lifecycle of crypto trading activity, including account funding, trading patterns, post-trade asset movements, and withdrawals or transfers to external wallets. Effective monitoring programs combine traditional brokerage surveillance with monitoring of fiat transactions and include important on-chain risk indicators. The goal is not to create blockchain analytics systems within the bank, but to use on-chain signals in a controlled and clear way to generate alerts, conduct investigations, and escalate issues. Institutions must clearly document how on-chain indicators are used, what limitations they carry, and how analysts are expected to interpret probabilistic risk signals. Without proper guidelines, on-chain data can create additional confusion, bias, and issues rather than enhancing detection.

3 Sanctions:

The risk of sanctions in crypto trading goes beyond simple name-based screenings. Potential exposure can arise from indirect transactional connections, ongoing interactions with high-risk wallet clusters, or patterns of behavior linked to sanctioned jurisdictions or entities. An effective sanctions compliance framework should clearly outline the assessment processes for both direct and indirect exposure, establish escalation thresholds, and document the rationale for sanctions-related decisions. Institutions need to articulate how they achieve a balance between risk sensitivity and proportionality, ensuring that their sanctions controls are precisely calibrated to prevent both under-detection and over-responsiveness.

4 Governance Oversight:

Governance links all elements of a framework. Regulators now assess not only the presence of controls but also the reasoning behind their creation, testing, and management of limitations. This includes risk management for transaction-monitoring models, oversight of third-party analytics, justification of thresholds, and ongoing reassessment as crypto markets evolve. Programs lacking clear explanations of their design choices may receive negative findings, even if they are operationally mature.

Why Crypto Brokerage AML Programs Commonly Fail:

Many banks' crypto brokerage programs fail because they assume that existing brokerage AML frameworks can be easily adapted for crypto. This assumption creates significant gaps in post-trade monitoring and external exposure management as assets leave the institution.

Another common failure is over-reliance on third-party blockchain analytics tools without sufficient internal governance. Vendor outputs are inherently probabilistic and methodology dependent. Treating risk scores as deterministic conclusions creates challenges during validation, threshold setting, and regulatory review.

Operational complexity further compounds these issues. Travel Rule obligations, cross-border data constraints, and inconsistent counterparty standards introduce friction that many programs underestimate. Weak documentation, unclear exception handling, and inconsistent investigative narratives erode auditability.

Finally, even the best-designed controls can fail if the documentation does not keep up with their implementation. Under a defined documentation procedure, institutions must clearly communicate their control intentions, limitations, and effectiveness. Failing to do so can lead to findings that are disconnected from the actual risk outcomes.

Expertise Oversight:

How Davies Can Support You:

The gap between traditional brokerage Anti-Money Laundering (AML) expertise and effective execution in crypto brokerage stems from the need for specialization. The crypto landscape presents unique technical and regulatory challenges that require in-depth knowledge. A seasoned crypto AML specialist can translate on-chain activity into risk frameworks, aligning controls with governance requirements and streamlining market entry.

Davies assists banks, brokerage firms, and fintech companies in implementing crypto brokerage AML by defining operational models, creating tailored frameworks, and providing documentation for examiners. They also offer independent validation to assess monitoring effectiveness, positioning themselves as a strategic partner for responsible innovation in the crypto space.

References (Public Sources)

- Office of the Comptroller of the Currency (OCC). Interpretive Letters on Crypto Asset Activities and Riskless Principal Transactions.
- Financial Action Task Force (FATF). Targeted Updates on the Implementation of the FATF Standards on Virtual Assets and VASPs.
- Financial Crimes Enforcement Network (FinCEN). Guidance on the Application of the Bank Secrecy Act (BSA) to Virtual Currencies.

Author :

Kunal Bavishi
Principal Consultant
E: kunal.bavishi@davies-group.com

Office location:
99 Madison Avenue, New York,
Ny 10016, United States

Davies US LLC

Davies US LLC. Registered office: 135 Allen Brook LN STE 101, Williston, VT

Disclaimer and Copyright Notice

11145709459_03_26_Executive Search - Brochure - Spec Serv_v1_MB