The Intersection of AML and Sanctions on Digital Assets

October 31, 2025

Digital assets have created new opportunities for innovation, but they also present a growing challenge for regulators and compliance teams. The intersection of AML (anti-money laundering) and sanctions on digital assets is becoming one of the most pressing issues for financial institutions and crypto service providers. Can compliance frameworks keep pace with the borderless and pseudonymous nature of cryptocurrencies?

Governments and regulators are treating digital assets with increasing scrutiny. The Financial Action Task Force (FATF) has extended its AML standards to virtual asset service providers (VASPs), requiring them to apply customer due diligence, transaction monitoring, and Travel Rule, which mandates information sharing between entities involved in transfers. At the same time, sanctions authorities such as the U.S. Office of Foreign Assets Control (OFAC) and the EU have been blacklisting crypto wallets linked to illicit actors, including ransomware groups and entities circumventing international restrictions. This dual focus means organizations must treat AML and sanctions obligations as interdependent rather than separate silos.

Why AML and sanctions converge in crypto

AML and sanctions intersect most visibly in cross-border digital asset transactions. Unlike traditional finance, crypto networks operate 24/7 and do not rely on

intermediaries with well-established compliance procedures. This creates vulnerabilities: sanctioned actors can attempt to launder funds through mixers, decentralized exchanges, or privacy coins. For compliance teams, the same tools used for AML—such as blockchain analytics, wallet screening, and suspicious activity reporting—are increasingly applied to sanctions enforcement.

This convergence is also driven by geopolitical dynamics. Recent conflicts have shown how digital assets can be used to evade restrictions, leading to heightened enforcement pressure. Financial institutions, even those with limited direct exposure to crypto, face secondary risks if they process fiat on- and off-ramps connected to flagged addresses. As regulators tighten expectations, the line between AML obligations and sanctions compliance becomes blurred, requiring integrated approaches.

Practical implications for compliance programs

Institutions now need robust frameworks that cover both AML and sanctions in digital assets. This begins with comprehensive KYC (know your customer) processes that capture wallet ownership details and beneficial ownership where possible. Transaction monitoring must extend beyond fiat movements to blockchain activity, leveraging advanced analytics to detect links with sanctioned addresses or high-risk typologies.

Another practical step is aligning internal governance. Too often, AML teams and sanctions teams operate separately, but digital assets demand joint expertise. Collaboration with blockchain intelligence providers and regulators is essential to interpret emerging risks, such as the use of decentralized finance (DeFi) protocols that lack clear accountable entities. Training staff to understand crypto-specific red flags—such as rapid layering across multiple tokens—is equally important.

The way forward

The convergence of AML and sanctions on digital assets is not temporary—it reflects the broader evolution of financial crime risk. While digital assets offer efficiency and inclusion benefits, their misuse can undermine global security and financial integrity. For compliance leaders, the priority is not just adopting new tools, but embedding a mindset that treats AML and sanctions as interconnected defences. The institutions that succeed will be those that anticipate regulatory shifts and invest in cross-domain expertise.