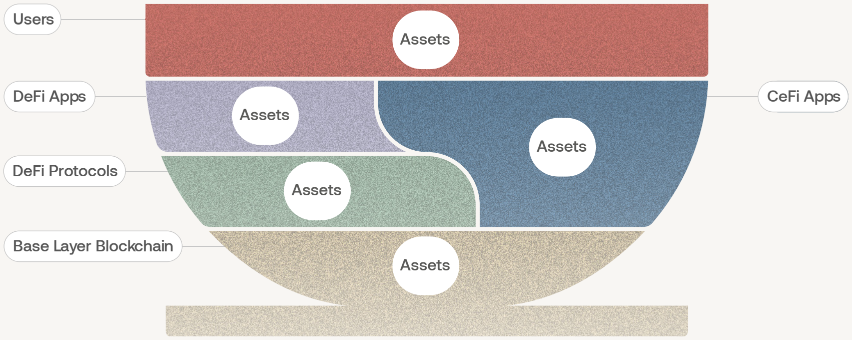
Crypto
Council for
Innovation

Crypto Illicit Finance Risk Management Guide

Crypto Asset Ecosystem Bowl



	Stack	Examples	Illicit Finance Risk Management Measures	Key Actors	Available Tools
●	CeFi Apps	Centralized exchange, centralized stablecoin issuer	AML/CFT Compliance program, including Know-Your-Customer (KYC) requirements; cybersecurity checks	CeFi App business compliance team	Transaction monitoring, sanctions screening, blockchain analysis
●	DeFi Apps	Self-hosted wallet browser app, app interface for decentralized exchange (DEX)	Wallet risk screening; cybersecurity checks	DeFi App business or organization	Transaction monitoring, wallet sanctions screening, blockchain analysis
●	DeFi Protocols[1]	DEX, lending protocols	Safety & soundness certification, including cybersecurity checks	Foundation or Decentralized Autonomous Organization (DAO), 3rd-party analysis firms, standardization bodies	3rd-party transaction analysis, proofs of status[2], smart contract audits
●	Base Layer Blockchain[1]	Bitcoin blockchain, Ethereum blockchain	Safety & soundness certification, including cybersecurity checks	Foundation or DAO, 3rd-party analysis firms, standardization bodies	3rd-party blockchain analysis, proofs of status[2], smart contract audits

For Illicit Finance Measures, blue text indicates indicates a measure that is newly developing or needs standardization

- **Centralized Finance (CeFi) Apps** are financial software applications directly managed by persons or legal entities that allow users to buy crypto products and services. They are controlled by a single entity that can work with law enforcement and other government entities to counter illicit finance.

- **Decentralized Finance (DeFi) Apps** are applications that facilitate users' access to DeFi protocols, allowing users to engage in financial activities such as lending, borrowing, and trading without relying on a centralized intermediary. They are businesses or organizations that can work with law enforcement and other government entities to counter illicit finance.

- **DeFi Protocols** are the underlying code or set of smart contracts that establish the programmable logic to facilitate decentralized financial activities. They are built on base layer blockchains and define the rules for operations and interactions such as cryptoasset issuance, use, transfer, and exchange. As purely self-executing software, DeFi protocols are unable to function as legal entities.

- **Base Layer Blockchains** provide the underlying infrastructure for decentralized activities by establishing consensus among all participants through the use of a public ledger and serving as a settlement layer. As purely self-executing software, base layer blockchains are unable to function as legal entities.

[1] For protocols and base layer blockchains, industry-driven certification standards should be developed to help establish best practices, set objectives for developers to build toward, and help consumers distinguish between well-designed protocols/blockchains and those that have yet to meet industry standards. As part of a risk-based approach, certification should be reserved for protocols and blockchains with significant volume and/or user base (e.g., > $50 million total value or 100,000 users). *See* CCI's Key Elements of an Effective DeFi Framework.

[2] We define "Proof of Status" as cryptographic evidence that a user's assets belong to a certain predefined category, such as not emanating from known thefts. Possible tools that may use or generate a proof of status include privacy pools and pre-transaction computation. Privacy pools are smart contract protocols that allow users to demonstrate that their funds originated from a pool of licit funds (i.e. "association set") without revealing their entire transaction history. Pre-transaction computation creates the capability of implementing transaction-specific policies for smart contracts (such as asset flows to avoid, dynamic inclusion/exclusion lists, etc.) in a decentralized manner. Such tools are not required, but could be employed by developers who want to offer such functionality for illicit finance risk management.

Questions? info@cryptoforinnovation.org