TRM GUIDE

MAY 2025

The Complete Crypto Compliance Program Guide for Financial Institutions

A practical roadmap for identifying crypto exposure, assessing risk, and building defensible compliance programs

TRMLABS.COM

Contents

Introduction

Cryptocurrency is no longer a niche sector within the global economy — it's a force reshaping financial services and commerce. As adoption accelerates and crypto transactions increasingly intersect with traditional banking rails, compliance teams face mounting pressure to keep pace. **But the biggest risk isn't exposure to crypto — it's not knowing you're exposed at all.**

This guide is designed to help financial institutions answer a few key critical questions:

- What does crypto exposure look like across your institution (and how can you manage that risk responsibly)?
- What are the key steps every financial institution should be taking to maintain compliance and ensure the licit exchange of crypto assets?
- How can financial institutions best engage with regulators as they begin thinking about a digital asset strategy?

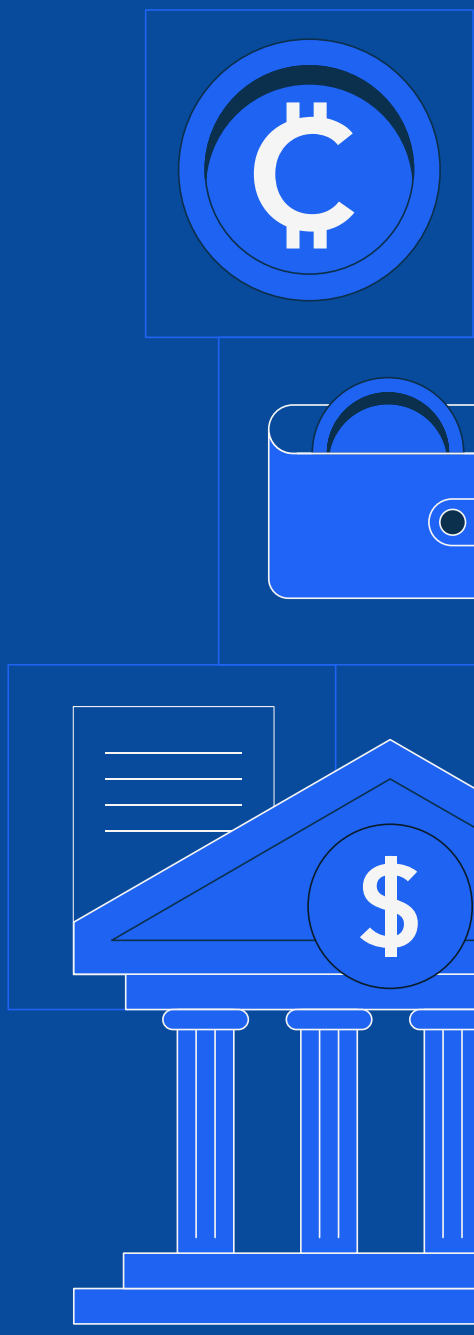
From wire transfers linked to digital asset businesses, to due diligence on high-net-worth crypto customers, we'll walk through actionable frameworks and intelligence-led best practices that empower compliance teams to navigate this evolving ecosystem with confidence.

Whether your institution is cautiously curious or actively engaged in digital asset services, this guide will help you build a defensible, risk-based approach that's both regulator-ready and future-facing.

QUICK LINKS

CHAPTER 1

Wires to wallets: Understanding and investigating wire exposure to crypto



In the fall of 2022, the US Secret Service (USSS) began an undercover investigative operation to disrupt an international money laundering syndicate. The syndicate was operating a particular type of virtual currency investment scam[1] that is oftentimes thought to take place solely within the crypto ecosystem. However, the reality is that these scams are often more nuanced.

In the course of the USSS's operation, an undercover agent began communicating with a fake customer service department run by the perpetrators. Syndicate operatives directed the agent to wire funds to an account in the name of a shell company called "Sea Dragon Remodel Inc.[2]," at a US banking institution. Law enforcement ended up uncovering over 60 shell accounts like this account – held at various banking institutions that were being used to launder the scam proceeds – and identified over 150 victims who had lost money to just this one criminal syndicate. The USSS also uncovered other fund transfers that were part of the scheme and were affected through cryptocurrency accounts.

Two truths emerge upon examining this and dozens of similar law enforcement cases like it.

First, **criminals don't exclusively use one type of asset to carry out a scheme and launder funds**. The "Sea Dragon Case" involved not only the use of wire transfers and crypto, but checks and credit cards, too. Ultimately, criminals will use any and all financial instruments available to them to exploit our financial systems. This multi-asset laundering approach necessitates a multi-asset compliance defense.

Second, **since the early days of Bitcoin, there has been an indirect relationship between traditional financial institutions (FIs) and crypto**. For FIs, that point of connectivity often arises through wire transfers to or from crypto-linked entities. The crypto nexus via wire transfers may stem from any number of sources, including customers taking the following actions:

- Wiring funds to exchanges
- Wiring funds to accounts held for custodians or stablecoin issuers
- Purchasing hardware for crypto mining equipment
- Transferring money to asset management firms investing in blockchain technology platforms or crypto assets

QUICK LINKS

[1] This type of scam has been referred to in the industry as "pig butchering," yet this terminology focuses on the exploitative process of these particular scams rather than the critical need to safeguard victims and educate financial institutions about prevention. FinCEN refers to these scams as virtual currency investment scams (https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf).

[2] https://storage.courtlistener.com/recap/gov.uscourts.vaed.539729/gov.uscourts.vaed.539729.1.1.pdf and https://coingeek.com/us-seizes-45-million-in-fraud-proceeds-from-tether-ftx-bank-deltec/

The growing link between banks and crypto

It's important to keep in mind that from a risk tolerance perspective, **not all wires with crypto-linked entities are part of illicit schemes**. Bitcoin is currently on a meteoric rise, pricing close to USD 100,000 at the time of this writing – and investors are taking note. In addition to growing institutional adoption, a recent Pew Research Center survey found that 17% of US adults (approximately 58 million people) had invested in or used cryptocurrency. Among men aged 18 to 29, this figure was notably higher, exceeding 40%.

Such significant activity doesn't happen without wire transfers. **Banks will be increasingly linked to crypto, and wire transfers have long been the primary nexus point between the two**. Moreover, banks that have historically derisked and blocked customer transactions with these entities will find it increasingly difficult to continue on that path as both retail and institutional involvement expand.

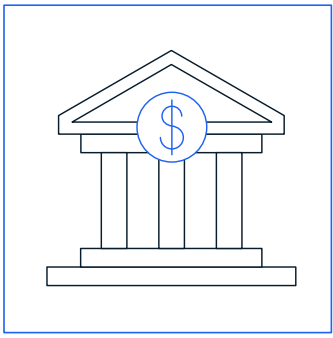
The duality facing banks and their compliance teams is clear: What do we do about wire transfers with crypto-linked entities? How should we balance the risks that dominate the headlines and are inherent to that space, while simultaneously managing growing interest from both Main Street and Wall Street? The question for banks is no longer *if* they should scrutinize these transactions but *how*.

Understanding crypto-linked entity activity

When learning about crypto and digital assets, one of the most important lessons is that this technology and its applications are not monolithic.

"Crypto" is not a single entity or activity – and it is far from uniform. Bitcoin is not the same as USDC. And NYDFS registered exchanges are not the same as overseas OTC services. In recent TRM Talks episodes, thought leaders from Standard Chartered, Fidelity, and Citi have all spoken not only about the dynamic nature of this ecosystem, but how financial institutions are building within that ecosystem.

The same applies with wire transfers involving crypto-linked entities. This sprawling ecosystem includes many types of entities, applications, and varied business purposes for the underlying wire transfers – many of which go beyond mere speculative trading.



Types of entities and activities

Mainstream news headlines often focus on activity that takes place with crypto exchanges (e.g. Coinbase, Binance, FTX, etc.), but there are many other types of entities and activities – a fact that was also noted by the Wolfsberg Group in their recent digital asset FAQs. These include:

- Over the Counter (OTC) services for institutional investors that serve as digital asset market makers
- Venture capital and other private investment activity funding digital asset startups
- Subscription and/or redemption activity from digital asset Exchange-Traded Funds (ETFs) and/or Exchange-Traded Products (ETPs)
- Blockchain technology computing equipment used for mining or staking services

Customers may use these and other crypto-linked entities and wire transfers for various legitimate purposes, such as:

- **Investment:** Seeking exposure to digital assets as part of a diversified portfolio
- **Trading:** Accessing crypto markets for short-term speculation or arbitrage
- **Payments:** Using dollar-backed stablecoins to facilitate remittances or corporate financial needs
- **Inflation hedge:** Converting fiat into digital currencies like stablecoins to preserve value in uncertain economic conditions
- **Private funding:** Using cryptocurrencies for personal or business transactions, especially across borders
- **Business expansion:** Institutional clients exploring blockchain technology or integrating crypto solutions into their operations

Red flags in wire transfers with crypto-linked entities

Of course, this space is not without its share of risks. And not all wire transfers to crypto-linked entities are benign.

A recent bank enforcement action – in which FinCEN noted specific instances of large volumes of wire transfer flows to crypto-linked entities that were insufficiently investigated – serves as a gripping reminder that these interactions cannot be ignored. **Banks must remain vigilant and use a variety of controls and investigative techniques to ascertain the legitimate from the illicit, and evolve along with changing typologies.**

When investigating specific wire transfers and customer activity, here are some of the primary red flags to look out for.

> **Note:** Some of these typologies will help identify non-compliant and risky crypto-linked entities, and others will help identify higher-risk transactions with legitimate crypto-linked entities. These typologies can also be used to help configure more programmatic transaction monitoring rules to flag at scale.

Red flag 1: Rapid multi-exchange exposure

Though different exchanges may offer different assets and spreads, multiple wires to multiple crypto exchanges within a short timeframe can be indicative of layering and splintering tactics.[3]

Red flag 2: Unusual "For Further Credit" (FFC) instructions

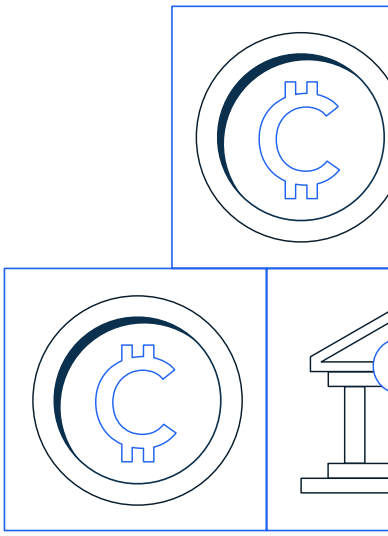
Unusual FFC instructions can indicate routing funds to unrelated or unexpected beneficiaries, potentially obscuring the ultimate recipient. This is a common tactic in money laundering schemes, including the case referenced above.

Red flag 3: Multi-product rapid movement of funds

Rapid movement alone is often not enough to identify illicit activity. But rapid movements coupled with multiple products (e.g. check deposit followed by wire to crypto exchange) in a single account is often a sign of atypical account activity. movements coupled with multiple products (e.g. check deposit followed by wire to crypto exchange) in a single account is often a sign of atypical account activity.

[3] Layering is when multiple wires and transactions are structured to obscure the path of the funds. Splintering is when funds are divided and sent to various exchanges to fragment the total amount and reduce the visibility of any single large transaction.

QUICK LINKS



Red flag 4: Increasing ramping amounts

A consistent theme heard from scam victims is that they transact with legitimate exchanges. Their investments start small, but then quickly increase over several weeks and months — eventually reaching significant sums.

Red flag 5: Outsized exposure vs. assets under management (AUM)

Customers wiring funds to crypto-linked entities much larger than their disclosed AUM or expected activity is indicative of money laundering risks, as recently seen in the FinCEN enforcement action noted above.

Red flag 6: Inconsistent cross-jurisdictional exposure

Customers wiring funds with crypto-linked entities that have a jurisdictional profile that doesn't align with the customer's background (e.g. retail company based in US, sending wires to exchanges in multiple other jurisdictions).

Red flag 7: Inconsistent business purposes

Business purposes that don't align with the counterparty's services (e.g. a "crypto investment" to a crypto payment processor service) indicate suspicious intentions behind the transfer.

Red flag 8: Unregistered intermediaries

For example, FTX customers were told to wire funds to an unregistered money services business (MSB) that was not in the name of FTX, and which did not have any apparent connection to FTX. This could itself be a red flag. And even if it is a benign investment, there are still anti-money laundering (AML) / combating the financing of terrorism (CFT) risks associated with transacting with a non-compliant exchange.

Conducting due diligence on crypto-linked entities

AML investigators may well recognize that these red flags are similar to traditional transaction monitoring red flags. Still, determining whether a single or group of wire transfers with a crypto-linked entity is legitimate requires context, nuance, customer background information — and a wider look at the account activity.

QUICK LINKS

While similarities exist, the transactional red flags analysis should be coupled with conducting counterparty due diligence on the crypto-linked entity itself — as this space presents some unique risks and unique risk mitigation techniques for crypto-linked entities. Evaluating the risk profile of crypto-linked entities is an essential component of monitoring wire transfers with these entities.

Six key considerations for risk assessing crypto-linked entities involved in wire transfers

Consideration 1: Where is the crypto-linked entity's jurisdictional footprint?

Determine where the crypto exchange operates, and whether it services customers or entities in high-risk jurisdictions like Russia — as threat actors (and thus suspicious wire transfers) have concentrated financial flows to these jurisdictions.

A recent report from TRM Labs found that Russian-speaking threat actors from across the former Soviet Union consistently drive most types of crypto-enabled cybercrime, from ransomware to illicit crypto exchanges and darknet markets. And from a sanctions exposure perspective, inflows to just one Russia-based crypto exchange, Garantex, accounted for 82% of crypto volumes belonging to all sanctioned entities internationally.

Consideration 2: What is the crypto-linked entity's licensing and regulatory posture?

Confirm whether the entity, where relevant, holds appropriate licenses and registrations consistent with their jurisdictional footprint.

For example, ascertain whether the entity meets the US regulatory definition of a money services business (MSB) if it operates inside the US or has US customers, and if so, whether it is registered with FinCEN. Does it comply with licensing requirements in jurisdictions such as Canada (under the Financial Transactions and Reports Analysis Centre of Canada), the United Arab Emirates (via the Abu Dhabi Global Market), or the European Union (through the Markets in Crypto Assets Regulation)?

Consideration 3: What is the risk appetite of the crypto-linked entity's crypto asset offering?

Assess the range of assets and services provided by the exchange, and consider whether it supports assets that are subject to greater exploitation by bad actors and scrutiny by regulators, such as privacy coins and mixing services.

Also, does it have standards for onboarding new assets? A large and unvetted asset offering can signal an exchange with a higher risk appetite, as well as a lack of stringent controls (and therefore a higher likelihood of being favored by threat actors).

Consideration 4: What parts of the crypto ecosystem does the crypto-linked entity service?

Analyzing the products and services a crypto-linked entity serves can provide signals about the levels of risk of any particular wire transfers with that entity.

For instance, consider crypto-linked entities that only serve institutional clients based in the US. These entities would naturally carry much less risk than one that services only retail customers from all over the world.

Consideration 5: Who are the crypto-linked entity's counterparties?

Similarly, you can ascertain a great deal about a crypto-linked entity by identifying who its primary counterparties are. Blockchain technology's transparency makes many of these connections visible and subject to analysis.

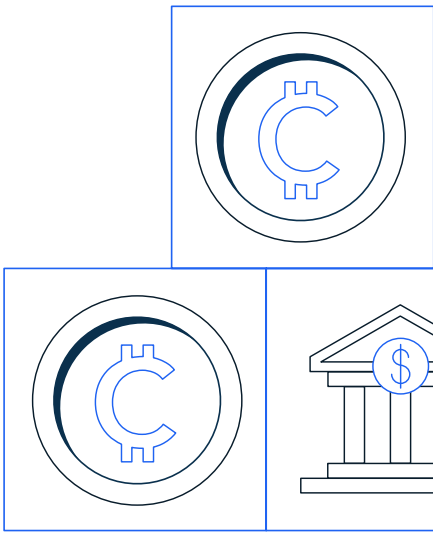
Consider, for instance, a crypto custodian whose major counterparties include high-risk exchanges, gambling shops, payment processors, retail OTC services, and other peer-to-peer services that can be more susceptible to being exploited by bad actors at scale. These connections can be a useful indicator to determine whether wire transfers with such entities might actually be problematic from a regulatory or reputational risk perspective.

Consideration 6: What is the effectiveness of the crypto-linked entity's AML/CFT and KYC controls?

Strong AML and Know Your Customer (KYC) controls are non-negotiable indicators of a crypto-linked entity's compliance maturity. But outside of reaching out to these entities, how can a compliance or risk professional get a sense of what a crypto-linked entity's internal controls are like?

The historical presumption has been that these entities operate on little to no controls. And while that may be true in select instances and countries, it may surprise traditional financial compliance officers how much their crypto compliance counterparts do to detect and prevent illicit activity. Additionally, blockchain technology provides unique ways to analyze the relative amounts of illicit risk flowing through a crypto-linked entity's pipes, which can serve as one indicator of the robustness of their AML controls.

QUICK LINKS



Weak controls – such as insufficient transaction monitoring or limited KYC processes – are more likely to lead to systemic exposure to Child Sexual Abuse Material (CSAM) vendor cashouts, sanctioned exchange exposure from Iranian exchanges, or large scam networks – all issues made visible by blockchain intelligence solutions and insights.

While the data needed to assess these factors may seem daunting to obtain, blockchain intelligence tools actually aggregate each of these data points and risk factors in a single solution, enabling compliance teams to incorporate this data into their investigative and diligence processes.

A balancing act: Vigilance and openness

Global cryptocurrency adoption is at unprecedented rates, driven by a myriad of economic, regulatory, and political forces.

This adoption comes with several key benefits for developing nations – including **greater financial inclusion** for unbanked and underbanked populations, **accelerated cross-border transactions, economic protection** in countries experiencing high inflation or currency volatility, and support for **vibrant tech and entrepreneurial ecosystems**.

Meanwhile, factors like the recent US election, fintechs like PayPal and Stripe embracing stablecoins, and traditional financial institutions like BlackRock and Fidelity offering crypto exposure are all factors that could significantly reshape and accelerate the future of cryptocurrency regulation globally.

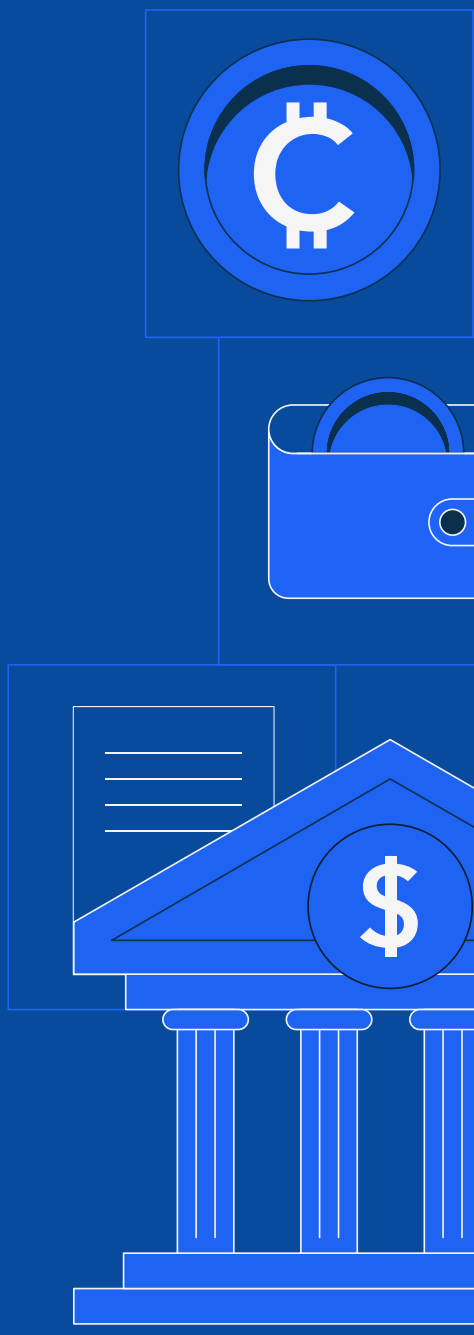
The growing adoption of crypto-related services will inevitably increase banks' exposure to digital assets. Navigating the intersection of wires and wallets is a complex but increasingly critical task for financial institutions.

Next, let's take a closer look at best practices for identifying crypto exposure across your institution – and how to leverage blockchain intelligence tools like TRM to mitigate your risk.

QUICK LINKS

CHAPTER 2

Identifying crypto exposure across your institution



The digital asset landscape continues to gain momentum every year. And growing global regulatory clarity, institutional adoption, a diversifying set of use cases, and a more positive stance from US policymakers and politicians under the Trump administration have all converged to drive surging interest in crypto and blockchain technology.

Against this backdrop, financial institutions now face a core challenge of identifying and assessing the myriad opportunities in digital assets. **Moreover, emerging regulatory expectations will continue to fall on institutions to undertake and document a thorough assessment of what that exposure looks like.** Institutions will continue to face heightened regulatory scrutiny – and an increased possibility of reputational risks for their crypto exposure – putting additional pressure on compliance teams to get it right.

Risk assessing current exposure

To mitigate the emerging regulatory and reputational risks from crypto-linked activities, institutions may look to develop and maintain a risk assessment process that identifies, analyzes, and mitigates risks stemming from their crypto exposure.

A prudent first step is a thorough evaluation of current crypto exposure and risks across various lines of business. This may include analysis such as:

Institution-wide risk assessment

- **Enterprise mapping:** Map every line of business intersecting with crypto (e.g. retail banking, commercial accounts, trading desks, etc)
- **Measure and analyze:** Determine how these various nexus points could introduce vulnerabilities (e.g. heightened potential for money laundering)
- **Existing controls:** Ascertain what existing controls may already mitigate some of these risks

Customer and transaction-level risk

- **Customer identification programs (CIP) and customer due diligence (CDD):** Integrate crypto-specific factors when verifying customer identity and conducting due diligence in order to capture and assess exposure at the onboarding stage. For instance, onboarding questionnaires may ask about whether there is material wealth from crypto activities.

- **Enhanced due diligence (EDD):** Apply stricter scrutiny to higher-risk crypto entities. For example, verify whether on-chain activity aligns with the stated purpose and expected transaction volume.
- **Transactional information:** Institutions may want to consider an assessment of crypto exposure across various payment channels or larger banking deals involving crypto entities.

Identifying use cases across the institution

Here's a list of areas across your institution where you may have either current crypto exposure, or potential areas where there may be future crypto exposure based on your institution's crypto strategy.

1. **Counterparty activity:** It is highly likely that your institution already has customers who transact – through your institution – with crypto entities
2. **Asset management:** Crypto businesses, such as cryptocurrency exchanges and mining firms, often seek to deposit fiat funds at traditional FIs for diversification or yield
3. **Private wealth:** High-net-worth individuals with substantial crypto-derived wealth may look to liquidate crypto assets and obtain private wealth services
4. **Investment banking and financing:** Crypto businesses often require traditional investment banking services for M&A, debt/equity financing, restructuring, or other capital market transactions
5. **Crypto-linked exchange-traded products:** Banks offering customers the ability to purchase digital assets like Bitcoin ETFs
6. **Securitized lending:** FIs may offer securitized dollar loans while accepting stablecoins or other digital assets as collateral
7. **Digital asset custody services:** Many institutions are considering custody solutions that enable customers to buy, sell, and transfer cryptocurrencies
8. **Tokenization:** Tokenizing real-world assets (e.g. bonds, private equity funds, and other securities) by placing traditional assets on the blockchain to expand market access and unlock liquidity through fractional ownership

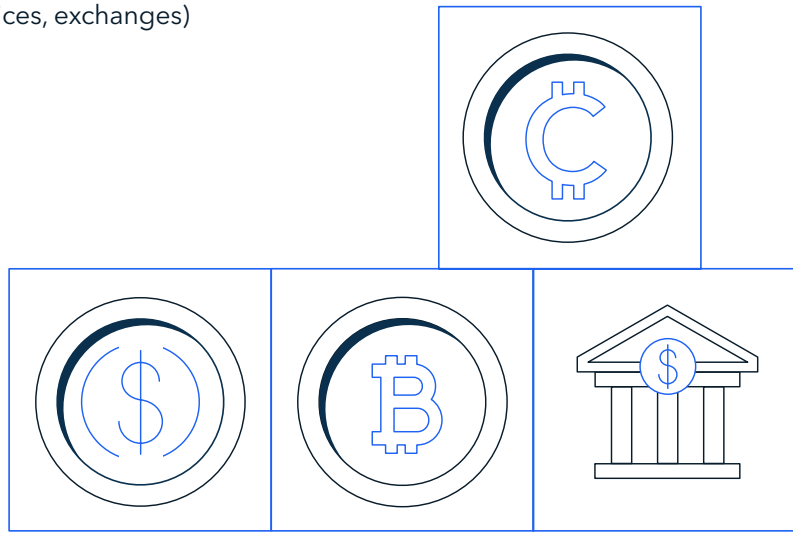
9. **Employee outside business activities:** With growing public interest in crypto, some employees may engage in personal trading or external crypto investment activity that may be subject to existing outside business activity policies

Leveraging blockchain intelligence to mitigate risk

Blockchain intelligence tools are incredibly versatile. The data and intelligence these platforms provide are just as valuable in helping authorities take down international money laundering networks as they are in helping financial institutions conduct enhanced due diligence on crypto entities.

In the process of evaluating your current risk exposure, as well as vetting future crypto opportunities, blockchain intelligence tools are a key component in helping compliance teams:

- Conduct risk assessments of crypto entities, factoring in the client's operating jurisdictions, regulatory status, and on-chain funding sources
- Verify the source of funds, ensuring consistency between a client's narrative and transparent on-chain activity
- Screen collateral and margin call deposits for crypto-linked lending for signs of money laundering or sanctions violations
- Analyze the sources from which Bitcoin ETF issuers purchase their liquidity
- Conduct end-to-end transaction monitoring of payment and withdrawal activity
- Assess the inherent risks of specific tokens, business projects, and counterparties involved (e.g. custodians, OTC services, exchanges)



Given the complexity of crypto markets and technologies, many FIs find value in forming cross-functional teams dedicated to digital assets. These "Centers of Excellence" coordinate strategy, enforce consistent risk controls, and act as training hubs – keeping compliance and operational teams on top of emerging threats, trends, and regulatory updates.

TRM in action

TRM enables FIs to identify unknown crypto exposure with **Entity Screening** – a comprehensive list of VASPs, including high-risk facilitators beyond exchanges. FIs can ingest this list via a flat file or API to cross-reference with their transaction monitoring data.

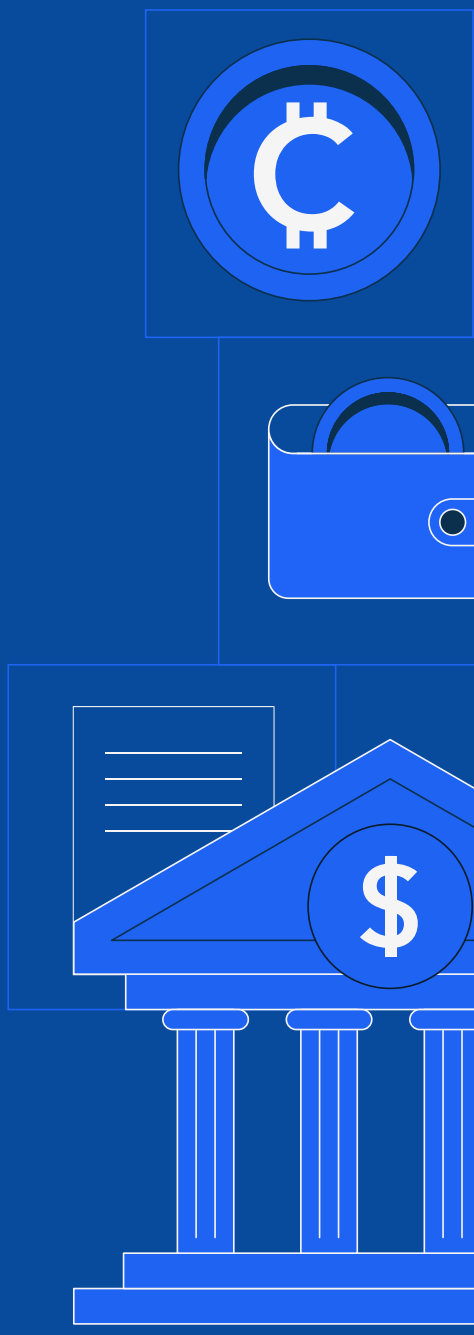

```
{
  "entity": {
    "entity_name": [redacted],
    "trm_urn": "7fa2ca3d-3c1b-4734-b1d0-d66f825465f2",
    "legal_name": "Moon Tech PTY Limited",
    "category": "Exchange",
    "country_of_supervision": [
      "United Arab Emirates",
      "France",
      "Bahrain",
      "Italy",
      "Spain",
      "Sweden",
      "El Salvador",
      "Poland",
      "Kazakhstan",
      "Australia",
      "New Zealand",
      "Thailand",
      "South Africa",
      "Lithuania",
      "Turkey",
      "India",
      "Argentina",
      "United Arab Emirates (ADGM)"
    ],
    "countries_restricted": [
      "Canada",
      "Netherlands",
      "United States",
      "Cuba",
      "North Korea",
      "Iran",
      "Syria",
      "Crimea",
      "Ukraine"
    ],
    "legal_name_jurisdiction": "Australia",
    "legal_name_reference": "98 621 652 579",
    "regulatory_status": "Licensed",
    "privacy_tokens": "Yes",
    "kyc": "Level 3",
    "entity_risk": "Low Risk"
  }
}
```


Now that you've identified potential sources of risk exposure to your financial institution, let's explore best practices for conducting due diligence on Virtual Asset Service Providers (VASPs) with a crypto nexus so that you can interact with them safely and effectively.

QUICK LINKS

CHAPTER 3

VASP due diligence: Onboarding institutions with a crypto nexus



Understanding the risk profile associated with Virtual Asset Service Providers (VASPs) is critical for conducting customer due diligence, enhanced due diligence, and ongoing customer monitoring. Additionally, adopting a consistent diligence framework for all crypto entities — regardless of what business line the relationship stems from — helps achieve consistent outcomes across your institution, provides guidance for non-compliance personnel prospecting VASPs, and mitigates regulatory and audit risks.

> **Note:** No one factor may be determinative on whether to onboard an entity or not. Rather, the exercise enables compliance teams to have the maximum amount of context and data available to make the best decision that fits within their risk appetite.

Understanding the VASP ecosystem

The VASP ecosystem is complex and dynamic. VASPs encompass a broad range of businesses that facilitate cryptocurrency transactions — including exchanges, custodians, OTC brokers, peer-to-peer (P2P) platforms, and decentralized finance (DeFi) protocols. Each carries its own risk profile and expected activity to monitor against.

Given this variability, financial institutions must assess a range of risk factors for the VASP in order to determine whether it falls above or below the institution's risk tolerance level. These include considerations like a VASP's:

- Jurisdictional footprint
- Licensing status
- Exposure to financial crime risks

Without proper due diligence, engaging with a non-compliant or high-risk VASP can expose financial institutions to regulatory scrutiny, financial crime risks, and reputational damage. However, with the proper tools and framework, financial institutions can safely engage with these entities and mitigate risks.

Five factors to consider for VASP due diligence

Here's a breakdown of five factors to consider when conducting VASP due diligence.

Factor 1: Understanding the jurisdictional footprint

Institutions may examine whether the crypto entity operates exclusively in one jurisdiction, globally, or within high-risk jurisdictions where AML controls may be weak or nonexistent. The presence of operations in such locations raises issues around

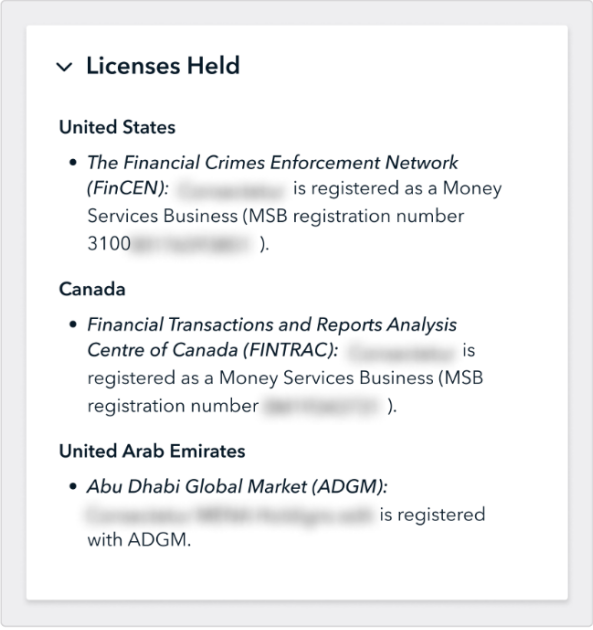
regulatory arbitrage, where firms exploit gaps in oversight to conduct business with minimal compliance obligations. A global exchange, for example, does not directly imply that the entity is too high-risk to onboard; rather, it raises the bar for what risks need to be mitigated and reviewed as part of the diligence process.

Institutions can derive the jurisdictional footprint of a crypto entity by looking at its legal entities, fiat currency support, and licensing status — and by viewing major counterparties via on-chain transactional flows to determine where customers may be located.

Factor 2: Verifying regulatory licensing

Institutions should confirm whether the entity holds the necessary licenses or registrations to transact in the jurisdictions it operates in. For instance, in the United States, a VASP facilitating crypto transactions is likely required to register with the **Financial Crimes Enforcement Network (FinCEN)** as a Money Services Business (MSB). Firms operating in Canada must register with the **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**. And firms within the European Union will now be required to be compliant with the **Markets in Crypto Assets (MiCA)** regulation.

Failing to maintain proper licensing and registration exposes not only the VASP, but also its banking partners, to regulatory and reputational risks. Institutions should conduct thorough reviews of registration statuses and, where possible, validate licensing details.



TRM Know-Your-VASP tool

QUICK LINKS

Factor 3: Assessing the type of crypto services

Compliance officers will be familiar with the adage: "If everything is high-risk, nothing is high-risk." And certainly not all crypto ecosystem activity poses the same level of risk.

The specific nature of a VASP's crypto activities and products play a significant role in determining its level of risk exposure. For example, institutions may assess whether the VASP has retail or institutional-only customers, directly facilitates crypto transactions (such as enabling customers to transfer crypto assets to unhosted or private wallet addresses), or perhaps only enables trading of crypto products with no transactional capabilities.

Additionally, the level of connectivity between the VASP's on-chain activity and the financial institution also matters. A bank considering providing fiat on- and off-ramps for crypto exchanges and its underlying customer will naturally carry a higher risk profile than one providing financing to a VASP looking to acquire new businesses. Similarly, a bank considering whether it can provide asset management services for the VASP may scrutinize whether the funds being deposited at the bank represent (1) treasury funds that the VASP holds from revenue, or (2) more direct deposits from retail customers.

Identifying your organization's own risk appetite against these different services and level of connectivity will be a key determination that should be made in the early stages of building out your compliance program.

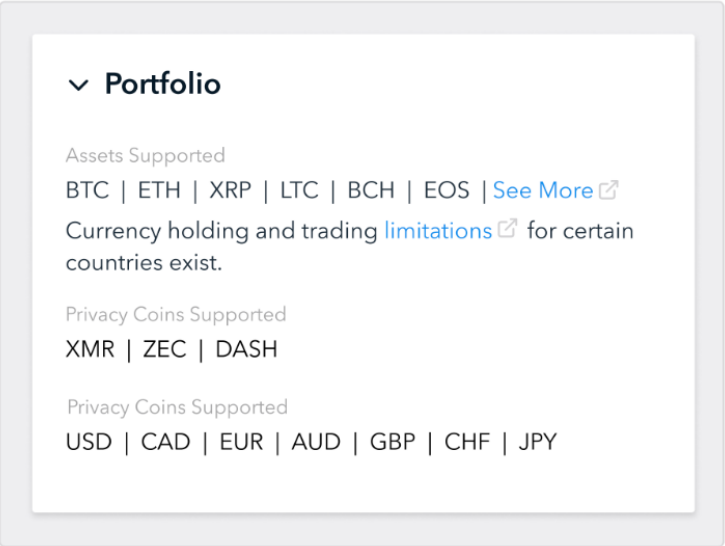
Factor 4: Assessing crypto asset offerings

The type of digital assets a VASP supports can offer valuable insights into its own risk profile, appetite, and tolerances. Financial institutions should evaluate whether the entity lists high-risk assets such as privacy coins (e.g. Monero), which are commonly associated with anonymity-enhancing features that complicate transaction monitoring.

Critically, an institution may also ascertain whether the VASP's privacy coin offerings are limited to trading only, or whether they permit customers to send these assets further on-chain via withdrawals or deposits – opening up increased money laundering risks. A VASP offering a wide range of tokens with limited vetting procedures may also present heightened risks. If an entity allows hundreds of token listings without stringent due diligence on new asset onboarding, it may indicate weak internal controls or an excessive risk appetite.

> **Note:** As noted previously, the presence of a large number of crypto asset offerings isn't wholly determinative of the VASP's level of risk. Rather, it requires that additional risk mitigation procedures be put in place in order for the organization to get comfortable where there is more risk.

QUICK LINKS



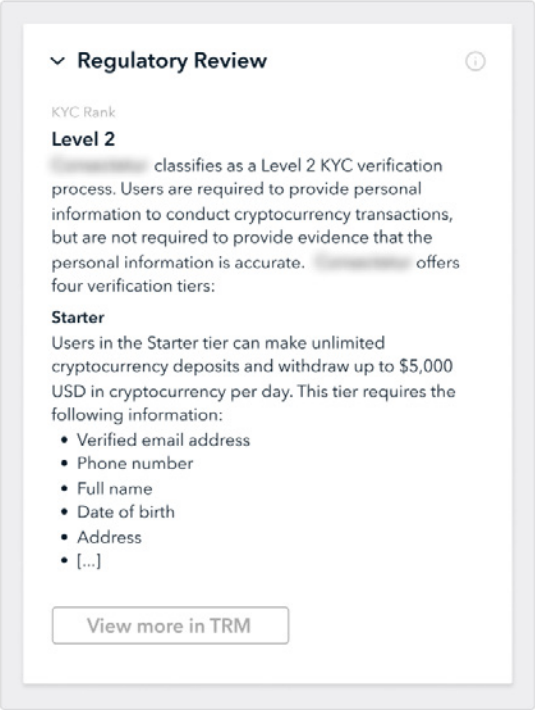
TRM Know-Your-VASP tool

Factor 5: Evaluating AML and KYC controls

A VASP's approach to AML and Know Your Customer (KYC) compliance is perhaps the most crucial diligence factor. Here's a list of questions you can ask to help assess how robust the controls are at a VASP:

- **Transaction monitoring:** Does the VASP have transaction monitoring controls in place for all of the crypto assets it supports? Or does it only cover a portion of the assets?
- **Sanctions screening:** Does the VASP screen customer information against global sanctions lists only at onboarding, or does it conduct ongoing screening on a periodic basis as well as all transactional activity?
- **Customer due diligence (CDD) and enhanced due diligence (EDD):** Does the VASP implement tiered verification processes based on risk levels? Are high-risk customers subjected to additional scrutiny? Do they require government identification to begin trading activity or just a name and email?
- **Compliance staffing and expertise:** Does the firm employ a well-resourced and experienced compliance team? Is there a money laundering reporting officer with commensurate experience given the products and services it offers?

Financial institutions should scrutinize these areas closely to determine whether the VASP's compliance posture aligns with their own regulatory obligations.



TRM Know-Your-VASP tool

Leveraging blockchain intelligence and Know Your VASP (KYV) tools

While traditional entity diligence relies heavily on open source information and responses from the prospect, VASP risk assessments require a deeper analysis which will often include blockchain activity.

Blockchain intelligence tools can provide data, helpful indicators, and evidentiary support for all of the factors listed above. By combining on-chain intelligence with off-chain regulatory due diligence, financial institutions can develop a comprehensive risk assessment framework, tailored to the unique risks posed by digital asset businesses. Blockchain intelligence tools can also enhance the ability to assess the riskiness of an entity by using more dynamic risk scoring methods, including analyzing both direct and indirect counterparty and transaction relationships.

Common characteristics among high-risk crypto entities

For traditional financial institutions, the highest risk exchanges in the world are also the easiest to identify. These are exchanges based in sanctioned jurisdictions or sanctioned themselves, don't conduct any forms of KYC, and have a high degree of transactional connectivity to illicit finance networks. Naturally, no financial institution

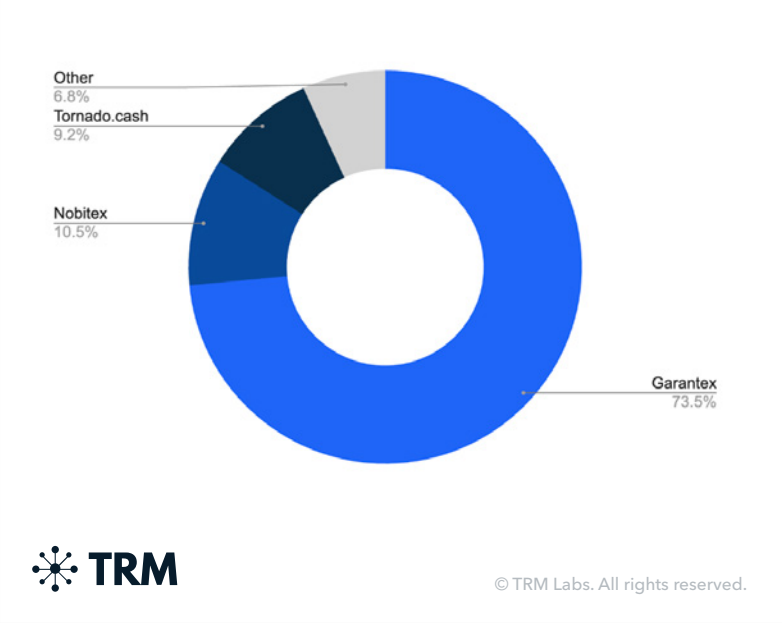
QUICK LINKS

would knowingly conduct business or activity with these entities. But if you remove those more obvious risky exchanges, what are the common factors among the next tier of more risky exchanges that financial institutions have a greater chance of connecting with?

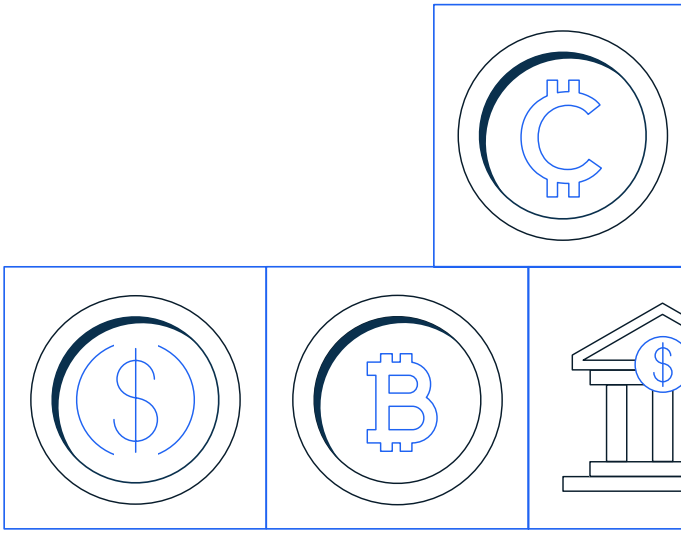
In a risk ranking analysis using TRM's blockchain intelligence, the following five factors were the most common characteristics among these high-risk entities.

Risk factor 1: Exposure to Nobitex/Garantex

Most of the highest risk exchanges in the world have significant counterparty exposure to **Nobitex** (the largest Iranian exchange) and/or **Garantex** (the largest Russian exchange, currently sanctioned). These two entities not only account for the vast majority of all sanctioned activity in the crypto ecosystem, but also, because of their size, serve as key liquidity points for a wide range of crypto activity — making connections to them more likely than smaller, less liquid exchanges. The higher level of exposure to these entities, the more likely there are gaps in their AML/sanctions controls.



Percentage of incoming volume by entity in 2024



Risk factor 2: Locations in offshore tax havens

Many high-risk exchanges may have incorporated entities in lower risk jurisdictions (e.g. a registered money service business in the US), but are based in locations that have historically been used as offshore tax havens. **The top highest risk exchanges are almost all based in either Mauritius, Seychelles, Hong Kong, or Saint Kitts.**

Risk factor 3: Licensing information

Unsurprisingly, most high-risk exchanges have some combination of either no licenses for jurisdictions they clearly operate in, licenses that have been revoked by authorities, or warnings from licensing authorities about the particular entity. Most compliant crypto exchanges over the past couple years have tried to course correct and come into compliance with licensing frameworks. Higher risk entities tend to lag behind and are much more likely to facilitate higher volumes of illicit activity.

Risk factor 4: KYC level as a proxy for illicit transactions

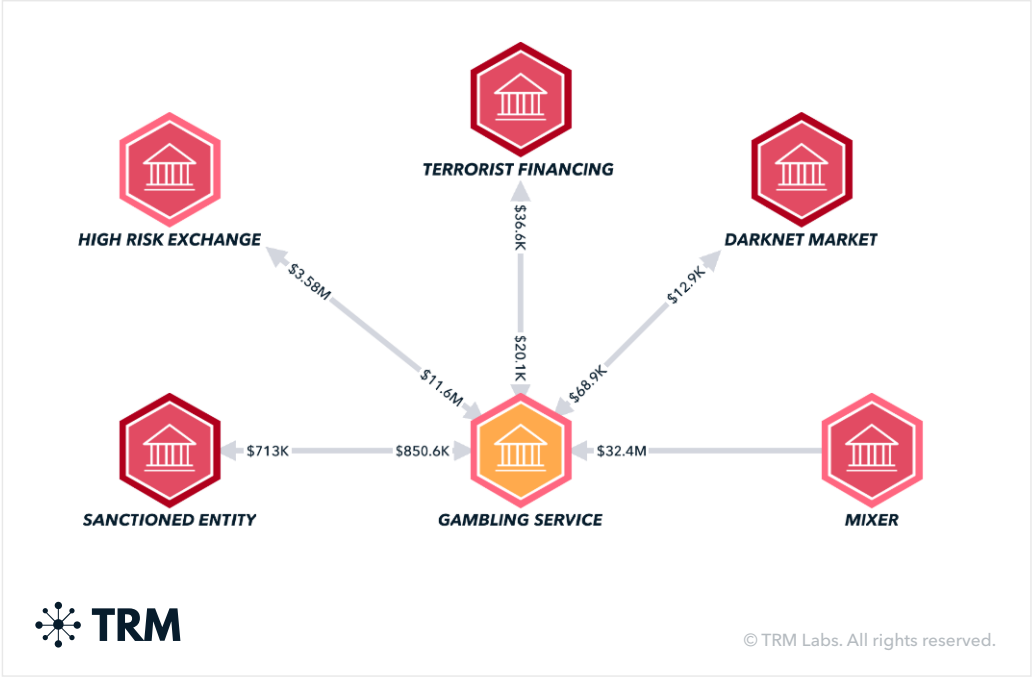
As TRM maps out different exchanges' risk profiles, we look to collect information about their KYC programs, where available. For example, do they require a government ID, or just a name and email? Again, unsurprisingly, there is a correlation between the amount of KYC an exchange collects, and the amount of illicit transactions flowing through the platform. This is due to bad actors being aware of the lowest barriers to entry, and seeking out these exchanges for on/off ramp activity.

While it is more likely that FIs will only evaluate a crypto entity with stronger KYC controls, reviewing the KYC levels of the most prominent counterparties of the target entity is a useful analysis to ascertain the strength of its compliance program.

Risk factor 5: Exposure to high-risk facilitators

High-risk facilitators are entities in the crypto ecosystem that operate as services, but have systemic amounts of illicit activity flowing through them. These may include retail OTC shops, payment processors, or gambling sites. Illicit actors use these services almost like a mixer: to obfuscate the flow of their funds since it is impossible to trace through services due to their omnibus account-like wallet infrastructures. Below is an example of what would otherwise appear to be a legitimate gambling company, but is actually an entity being used to facilitate transactions with high-risk actors.

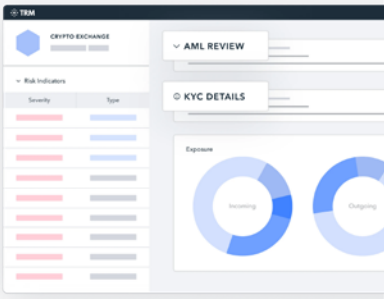
QUICK LINKS



Note: Ask about our **TRM Academy** training opportunities, where we walk through a case study of risk – assessing a VASP facilitating activity connected to drug cartels.

TRM in action

TRM Know-Your-Entity enables FIs to drill into comprehensive risk profiles for VASPs, including high-risk facilitators like OTC desks, payment processors, and cash-to-crypto. Every risk profile includes on- and off-chain data to empower FIs to make data-driven decisions during VASP onboarding, due diligence, and continuous risk assessments.

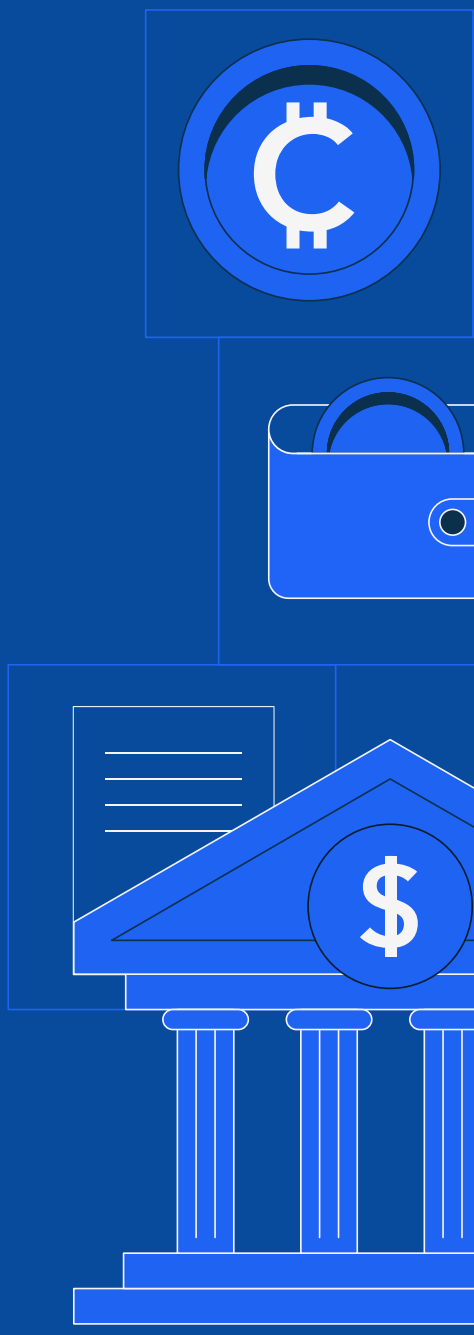


Next, let's take a look at the factors that are most helpful in conducting source of wealth (SoW) and/or source of funds (SoF) analysis. From gathering evidence of legitimate ownership and transaction histories to spotting early indicators of obfuscation techniques, we will explore how AML teams can augment their existing SoW and SoF processes using blockchain intelligence tools.

QUICK LINKS

CHAPTER 4

Source of wealth analysis for high-net-worth crypto prospects



For financial institutions operating under strict AML requirements, verifying a customer's source of wealth (SoW) from cryptocurrencies demands a combination of traditional due diligence and modern blockchain intelligence. This process goes beyond standard KYC and Customer Identification Program (CIP) checks, often requiring enhanced scrutiny of on-chain wallet activity.

Asking the right questions and establishing the narrative

Banking customers with crypto-linked sources of wealth may fall into one of two categories:

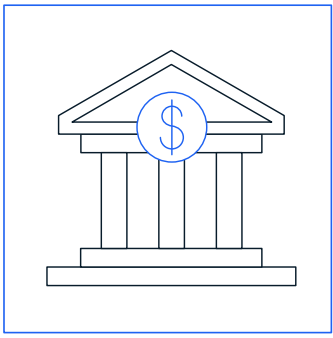
1. Prospects whose source of wealth stems from **traditional compensation or investment returns** involving a crypto entity. This may be an executive of a crypto exchange, a partner who works at a venture capital firm that invests in crypto, or a founder of a blockchain-linked company.
2. Prospects whose source of wealth stems from **trading, investing, or otherwise transacting more broadly** with direct crypto assets on-chain.

In the first instance, presuming the prospect was paid in traditional currencies, an on-chain analysis is likely not necessary – though it may be prudent to assess the risk of the crypto entity itself.

In the second instance, before delving into detailed on-chain analysis or requesting formal documentation or wallet addresses, it's crucial to ask targeted questions upfront that clarify how the prospect accumulated their crypto-related wealth – and the means by which they may liquidate it and bring dollars to your institution. **This narrative you collect from the prospect becomes invaluable as you look to ultimately verify whether their on-chain activity is consistent with their story.**

These questions may include:

- What cryptocurrencies are you liquidating?
- How did you acquire your cryptocurrencies (e.g. mining, ICOs, trading on a licensed exchange, staking, inheritance, etc.)?
- Over what time period did you accumulate these assets?
- Which platforms or exchanges have you used to trade or transact, and can you provide account statements or records if necessary?



- Do you control or utilize unhosted wallets? What specific wallet addresses do you use to conduct transactions, deposit funds at exchanges, trade in DeFi services, or make any transfers to other wallet addresses?
- Can you demonstrate that you control any private wallets holding this crypto?
- What proportion of your total net worth stems from crypto assets?
- Which crypto service are you using to liquidate your crypto assets?
- Have you reported your crypto gains for tax purposes?

Some prospects may push back on not wanting to provide this type of information. Here are some helpful tips for approaching those conversations:

- With some forms of wealth, we can validate the source through publicly available information (e.g. if someone sold a company, we may verify that through open source information). Depending on the specifics in this case, **an on-chain analysis may be the only way to actually verify the narrative we've been given**.
- **Regulatory expectations** require customers' source of wealth be verified.
- FATF guidance and some **regulatory statutes** (e.g. the US PATRIOT Act) require enhanced due diligence be conducted where there may be additional risk, and those steps often require the request of documentation.
- There is an emerging **industry standard**, as many institutions already do this today.

Gathering evidence of source of wealth

Once a narrative is collected and established, the next step is to collect verifiable evidence that supports the customer's narrative of generating wealth from cryptocurrency. **Since crypto assets and transactions often exist on public blockchains or exchange platforms, banks can leverage both traditional documentation and blockchain intelligence tools to bolster their source of wealth assessment.**

> **Note:** Depending on the facts and circumstances of the narrative, not all of these data points may be necessary.

Transaction records and wallet history

On-chain evidence

Ask for wallet addresses and on-chain transaction hashes that support the relevant transfers of the activity (e.g. if a customer is liquidating funds at an exchange and maintained assets in a private wallet, ask for the transaction hash that facilitated the transfer of funds from the private wallet to the exchange).

Example of wallet addresses and transaction hashes

Proof of ownership

In some cases, the customer can sign a message from their wallet to prove direct control. Alternatively, screenshots of wallet balances or exchange statements can serve as supporting evidence (though screenshots alone could certainly be falsified).

Exchange or platform statements

Trade statements and funding history

Request documented statements from major exchanges where the customer trades. Look for consistency between deposits, withdrawals, fiat conversions over time, and any potential transfers to other wallet addresses. If the customer has an extensive history of many years of trading and transacting in crypto, institutions may need to ascertain where a sampling approach may be sufficient, or perhaps ask more targeted questions over specific time periods. Here, institutions should be guided by a risk-based approach and consider other risk factors related to the potential customer.

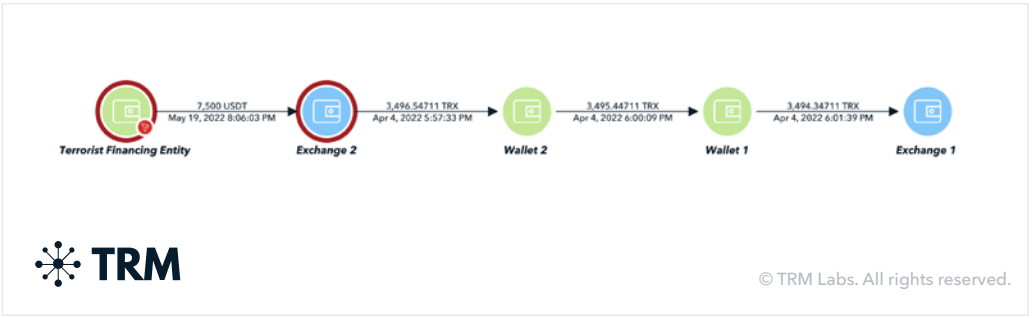
QUICK LINKS

On-chain analysis

When you begin to conduct an on-chain analysis, your goal is to verify that the prospect's story about their crypto wealth matches what you see on the blockchain, and to ensure you don't see any red flags. Here are some practical tips to keep in mind:

Tip 1: Be wary of tracing through services

As you trace funds back through different addresses in the SoF analysis, recall that one of the tenants of blockchain tracing is that, generally, **you cannot trace through a service such as an exchange, OTC desk, payment processor, etc**. This stems from the fact that crypto services often use omnibus or consolidated wallet infrastructures to manage customer deposits and withdrawal efficiently. Tracing through a service will likely cause an investigator to make incorrect assumptions about the validity of a source of funds path.



Exchange 1 is conducting a source of funds review on Wallet 1, who deposited funds to the exchange. If you attempt to trace back through Wallet 2 until you hit the Terrorist Financing Entity wallet, you will have traced through an exchange.

Tip 2: Explore exposure to a range of risk categories

In addition to reviewing whether the relevant wallet addresses have exposure to illicit finance risk categories (e.g. sanctions, terrorist financing, child sexual abuse material), **there may be exposure to other categories that, on their face, may not appear to be illicit – but may be inconsistent with what you would expect from the customer based on their narrative and background**. This may include things like individuals using OTC services, payment processors, gambling services, or other money transmitters that facilitate laundering services.

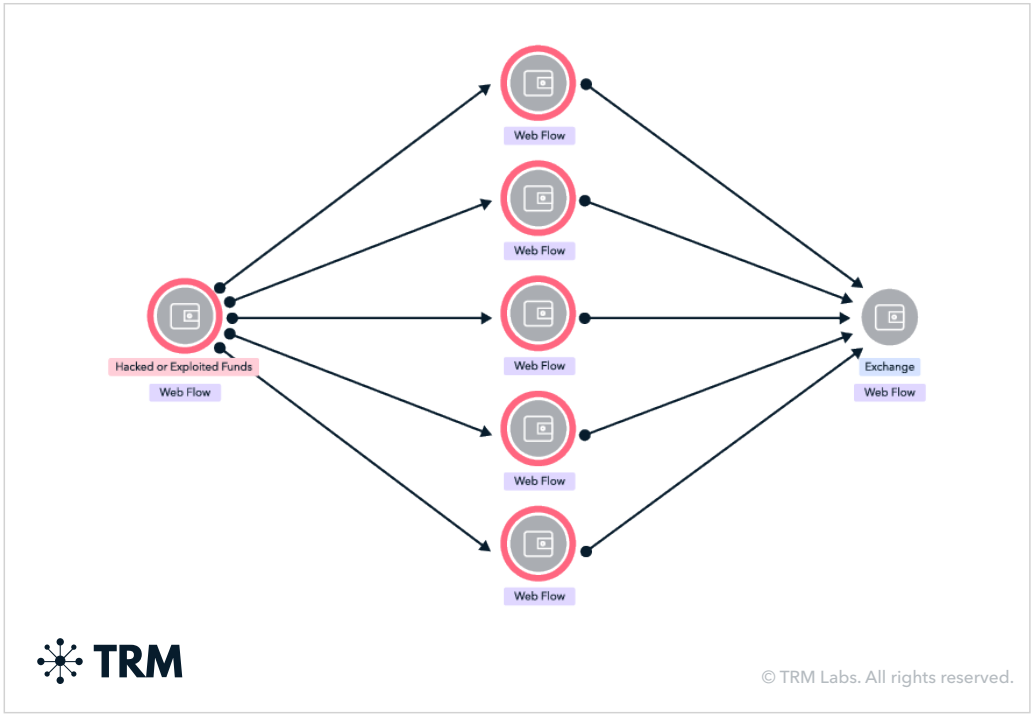
QUICK LINKS

Tip 3: Look at all data points to assess the holistic set of risks

Keep in mind that while blockchain intelligence tools excel at mapping bad actors and services to wallet addresses, there are other data points to consider as you analyze the flow of funds – including what services are used, the number of addresses used by a prospect, the timing of transfers, the type of assets they're using, patterns indicative of sanctions evasion, etc.

To assist users with monitoring for unusual patterns of activity, TRM pioneered the automatic identification of suspicious behaviors, called Signatures®, to automatically detect and trace behavioral anomalies that are often used as obfuscation techniques. The automatic detection and plotting of these patterns reduces the complexity and time needed for investigations.

These behaviors include not only **peel-chains** (i.e. small transactions are peeled off from the main flow of funds path and sent to other addresses or services) and **cross-chain swaps** (i.e. a technique used to swap one crypto asset for another without using an exchange), but other types of behaviors that are not normal and expected types of transactional activity.



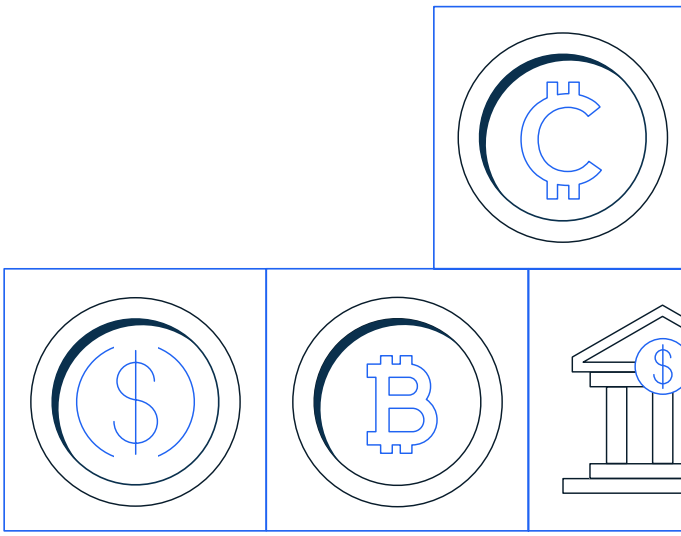
This obfuscation pattern shows an address that disperses funds to many addresses, before reconsolidating the assets back to a single wallet, in order to obfuscate the risk that the original wallet may be exposed to

QUICK LINKS

Red flag indicators

Here are some additional red flags to look out for in the course of your analysis:

- Use of services in higher risk jurisdictions or offshore tax havens
- Use of privacy coins, mixers, or other services that obfuscate the flow the funds
- Inconsistent or vague explanations (e.g. "early investor" with no documentation)
- Use of intermediary or single-use addresses with no other activity
- Frequently changing wallet addresses
- Large inflows from other unhosted wallets without a clear explanation
- Large deposit and sales of token projects that experienced dramatic price decreases following a sale
- Chain hopping without clear indication of why the swap of assets took place
- Swapping of tokens or NFTs back and forth between addresses (i.e. wash trading)
- Splintering funds across multiple wallet addresses prior to a deposit at an exchange
- Structuring transfers to circumvent certain reporting requirements (e.g. VCTR, daily limits for crypto ATMs, etc.)

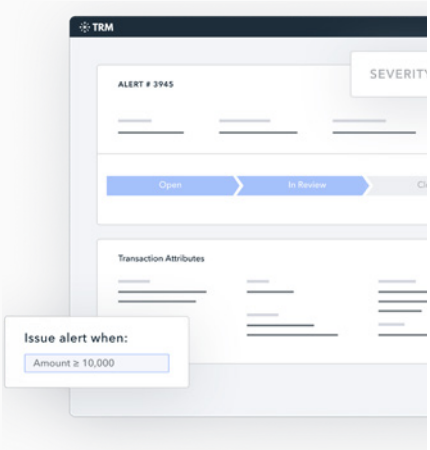


While it may seem daunting at first, by combining a prospect's narrative with diligent evidence gathering and careful on-chain analysis, you can build a robust source of wealth assessment process that supports regulatory requirements and protects your institution from bad actors looking to exploit it. Blockchain intelligence tools like TRM can accelerate the ability for compliance teams to conduct this kind of analysis by providing key red flag indicators and evidenced-based insights to the forefront of your team's analysis.

TRM in action

As FIs continue to adopt digital assets, blockchain intelligence will become a critical input to transaction monitoring workflows.

TRM Transaction Monitoring empowers organizations to detect risky transactions in real time, based on configurable rules to match internal threshold requirements.

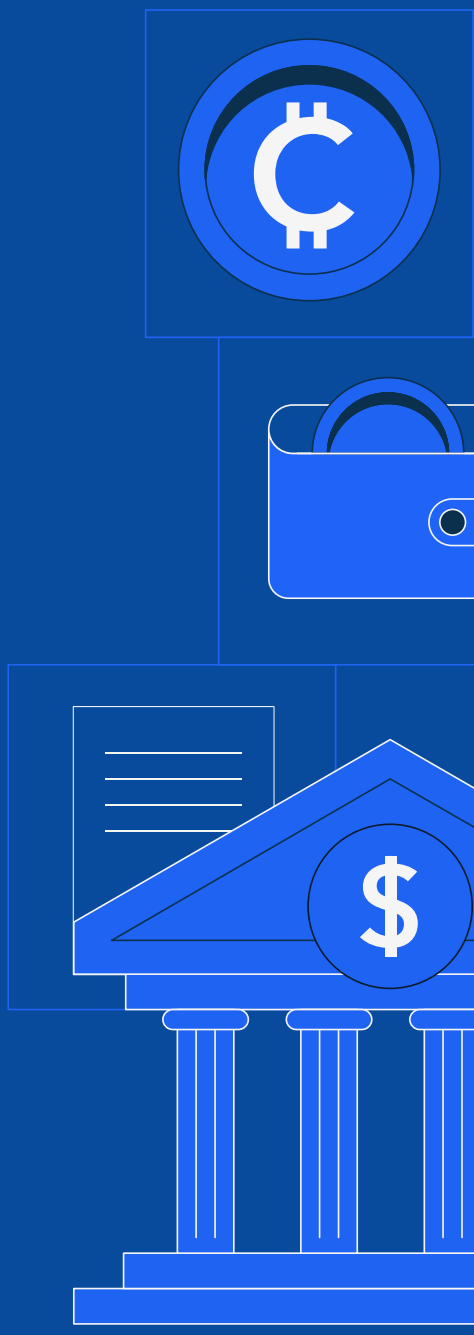


Finally, let's look at some best practices and tips for best engaging with — and navigating the expectations of — global regulators.

QUICK LINKS

CHAPTER 5

Best practices for navigating the regulators



Banks' journey into cryptocurrency began in earnest in the late 2010s, when a handful of institutions started exploring services like custody of digital assets and providing accounts for crypto exchanges. These early ventures were quickly met with a wary regulatory posture.

Bank supervisors, concerned about untested risks, often responded with more friction than facilitation. In some cases, this took the form of direct intervention. The Federal Deposit Insurance Corporation (FDIC), for example, quietly instructed two dozen banks to "pause" their crypto-related activities pending further review. These so-called "pause letters," later brought to light through FDIC records, signaled the extent of regulators' early skepticism.

Public supervisory statements from that period echoed a similar caution. In January 2023, the Federal Reserve, FDIC, and Office of the Comptroller of the Currency (OCC) issued a rare joint warning about crypto asset risks in banking. They pointedly cautioned that certain crypto activities were "highly likely to be inconsistent with safe and sound banking practices." The agencies catalogued a litany of concerns – from fraud and legal uncertainties to the volatility of crypto markets – and indicated a "careful and cautious approach" to any bank involvement in the sector.

Notably, regulators also stressed that banks were "neither prohibited nor discouraged" from serving lawful crypto clients. In practice, however, the tone of supervision was unmistakably guarded. **The early history of banks in crypto was defined by this push-and-pull: banks eager to innovate on one side, regulators pressing the brakes on the other.**

The Trump-era pivot

At the start of 2025, we saw global regulatory momentum around crypto accelerating – particularly in EMEA. The European Union's MiCA had entered into force, offering a comprehensive and harmonized framework for crypto oversight across the bloc. In the UK, the Financial Conduct Authority (FCA) expanded its registration regime and introduced stricter advertising standards for crypto firms. Meanwhile, the UAE and Switzerland continued to attract digital asset firms with clear licensing structures and pro-innovation regulatory sandboxes.

Against this backdrop of increasing international clarity, the United States stood at a crossroads – prompting the Trump administration to reevaluate its own posture toward banks and crypto.

From quarantine to competition

In the first few months of Donald Trump's second term, the administration launched a notable pivot in its regulatory posture toward crypto – one that departed from the

more cautious tone of the preceding years. Rather than treating crypto as a source of systemic risk to be quarantined, the new stance emphasized strategic engagement, competitiveness, and modernization of financial infrastructure.

Key agency appointments further catalyzed this shift. The Trump administration reinstated several officials with fintech and crypto expertise into prominent roles – most notably at the OCC, which issued updated guidance supporting the permissibility of crypto custody, tokenized deposits, and even certain staking services by federally chartered banks. This was a clear signal: the administration was not just allowing crypto activity – it was looking to build a stable regulatory home for it.

For banks, the Trump administration's 2025 pivot offered an invitation – though not a free pass – to engage in crypto, provided they did so transparently, compliantly, and in dialogue with their regulators. After years of mixed signals, banks now have a path to step into the arena – with clearer guardrails and a potential partner at the supervisory table.

That said, frontline examiners may still maintain some level of cautious skepticism about risks that the crypto ecosystem presents. **Bank compliance teams will have to effectively articulate and counter this skepticism by clearly explaining that they understand the business and services offered, the risks inherent in those activities, and that they've built out a robust environment to control for those risks.**

Tips for working with regulators

Given this history of initial friction and ongoing skepticism from supervisors, what can banks do to collaborate more effectively with regulators as they expand into cryptocurrency initiatives? Let's explore five actionable best practices compliance professionals should consider, drawn from regulatory guidance and real-world examples.

Tip 1: Engage early and proactively

Don't wait for regulators to discover your crypto activities. Rather, **inform them at the outset**. Banking agencies have made clear they expect early notification and dialogue around any crypto-related plans. In fact, each federal regulator has established processes for banks to engage in "robust supervisory discussions" about proposed crypto ventures.

By consulting regulators in the planning phase, banks can address concerns up front and avoid unpleasant surprises late in the building phase. Early, proactive engagement also builds trust and gives regulators confidence that a bank is approaching crypto in a controlled, transparent way.

Tip 2: Conduct thorough risk assessments

Before launching any crypto product or partnership, banks should rigorously assess the risks, be prepared to show regulators they have documented these assessments, and demonstrate that these risks are controlled for. This may include areas such as the bank's existing exposure to crypto entities, or, depending on the products and services, areas like fraud or volatility risk. Regulators will expect to see that proper **controls**, **gates**, and **guardrails** are in place for any crypto activity.

Additionally, robust risk management starts with board and senior management oversight. Ensure your board is informed and approving of the crypto strategy, and that detailed policies and procedures have been developed alongside the risk assessment. Document the results of your risk assessments and the mitigants put in place (e.g. capital buffers for crypto exposures, enhanced monitoring of transactions, triggers for escalation, etc.). By presenting regulators with a thoughtful risk analysis, banks signal that they are not venturing into crypto recklessly — but rather in a manner consistent with safety and soundness expectations.

Tip 3: Augmenting existing controls

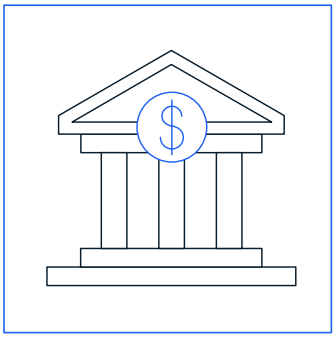
When launching crypto-related services, banks may feel tempted to build entirely new anti-money laundering (AML) frameworks from scratch. But creating standalone crypto compliance controls risks duplicating efforts, introducing inconsistencies with your existing program, and weakens the overall structure of your AML program.

For example, in one FDIC letter from mid-2023, a bank proposing to offer crypto custody services was explicitly cautioned that its plan to establish "a parallel transaction monitoring process" for crypto activities — separate from its core AML systems — could result in inconsistent oversight and gaps in suspicious activity reporting. The FDIC noted that "risk mitigation efforts must be coordinated within the bank's existing BSA/AML infrastructure" and warned against siloed compliance approaches that might undermine overall program effectiveness.

Instead, banks should **focus on extending and adapting their existing AML infrastructure.** There's no doubt that the crypto ecosystem introduces novel risks that may need to be controlled by novel tactics. However, institutions should endeavor to weave those novel tactics into their existing policies and procedures so as not to create fragmented programs.

This could mean integrating blockchain intelligence tools and checks into existing customer due diligence and enhanced due diligence procedures to fully assess the risks of crypto entities. Or, on a more granular level, this could mean ensuring that specific transaction monitoring processes (e.g. escalation guidelines, timelines for closing alerts, quality assurance rates, etc.) also apply to blockchain intelligence tools used to perform ongoing monitoring of activity for on-chain transactions and alerts.

QUICK LINKS



This approach ensures consistency, avoids internal silos, and allows compliance teams to operate within familiar frameworks — while still addressing new threats like blockchain obfuscation or peer-to-peer transfer risks. Regulators have made clear that AML compliance remains non-negotiable in crypto services, but they are more likely to support programs that demonstrate continuity with existing bank-wide controls.

Tip 4: Maintain open communication and documentation

Fostering an ongoing dialogue with regulators is key to a smooth relationship. Crypto markets evolve rapidly; as your bank's strategy or partnerships change, **keep your regulators in the loop.** Regular check-ins or status updates can preempt regulatory concerns before they fester.

It is equally as important to document all communications and understandings with regulators. If a regulator requests additional safeguards or a pause on a certain activity, follow up in writing to confirm the bank's commitments or the conditions to be met for approval. This creates an audit trail and helps avoid misinterpretation.

It's also critical to seek clarity rather than operate in ambiguity. For example, some banks that received the FDIC's crypto-related letters in 2023 were left in limbo: told to pause activities, but never explicitly given the green light to resume. To avoid such dead ends, banks should politely press for clear guidance on what would satisfy regulators' concerns. For example, by asking: "What specific controls or data would give you comfort for us to proceed?"

Open, two-way communication, backed by thorough documentation, turns regulatory supervision into a collaborative process rather than an adversarial one.

Tip 5: Embrace self-identification

As banks build out crypto-related programs, the instinct may be to perfect every detail before bringing regulators into the conversation. But waiting too long to disclose internal challenges can erode trust and lead to regulatory skepticism. Agencies like the FDIC, OCC, and OFAC have repeatedly emphasized the value of self-identification — where institutions **proactively flag gaps, delays, or missteps in their own crypto-related activities before issues are discovered during examinations.**

For example, if your team discovers that a planned blockchain analytics integration is delayed or a key crypto custody control isn't functioning as expected, this finding should trigger immediate internal escalation and timely communication with your supervisory contact. Regulators are often more focused on how a bank responds to problems than whether problems exist in the first place. Self-identified issues — particularly when accompanied by a clear remediation plan — demonstrate a mature risk culture and a willingness to take ownership. This builds credibility and can soften the tone of regulatory response.

QUICK LINKS

Conclusion

Crypto's integration with traditional finance is no longer hypothetical. Wire transfers, customer due diligence, investment services, and even custody offerings now frequently involve crypto-linked entities. Compliance teams that ignore these connections do so at their peril.

A few key points to remember:

- **Exposure is already here.** From wire activity to private banking relationships, most financial institutions already touch the crypto ecosystem — whether they know it or not.
- **Not all crypto activity is the same.** Differentiating between low-risk institutional players and high-risk facilitators is essential. A robust due diligence framework can help draw that line.
- **Traditional tools aren't enough**. Effective compliance in the crypto age requires enhanced risk assessments, blockchain intelligence, and a cross-functional approach.
- **Proactive engagement pays off.** Early regulator communication, consistent internal policies, and integration of crypto-specific tools into existing AML programs are critical steps toward building resilient programs.

At TRM Labs, we support compliance teams around the world in uncovering crypto exposure, conducting enhanced diligence, and staying ahead of regulatory expectations. To learn more about how TRM can help your institution build a safer, smarter crypto compliance program, explore our solutions or get in touch.

QUICK LINKS

Appendix

Centralized Finance	Key Characteristics	Purpose and Anticipated Activity
Financial Applications (examples)		
Centralized Digital Asset Exchanges (e.g. Binance)	Provide platforms for clients to buy/sell/hold or transfer digital assets. Mostly holders of money transmitter licenses	Provide on-ramp and off-ramp activities, holds client funds and facilitate transfers to private wallets
Custodians (e.g. Anchorage)	Provide secure storage of digital assets on behalf of their clients	Provide storage of client assets and execute transactions at the direction of the clients
OTC Trading Desks / Brokerage (e.g. Kraken OTC)	Connect buyer and seller for digital asset-related trading	Facilitate large private transactions that can be conducted as principal or agent
Proprietary Traders (e.g. Jump Trading)	Investment firm or vehicle uses their own money instead of seeking commissions from clients' trading	Acting as liquidity provider and trade digital assets using the company's own assets
Investment Funds (e.g. Grayscale)	Digital asset investment funds' primary objectives are to invest in digital assets and raise money from 3rd parties	Invest in both digital asset companies or crypto assets
Lenders (e.g. BlockFi)	Provide loans denominated in fiat currency or digital assets	Loans are highly collateralized and could involve digital assets in a variety of ways (e.g. collateral, margin payments, principal loan, etc)
Digital Asset Issuer (e.g. Circle)	Launch new tokens that can fund the creation of new blockchain-based services and support the development of new cryptoassets or cryptoassets-powered platforms	Issue new tokens to institutional investors or individual investors, facilitate payment and wallet storage features
Payment Processors (e.g. BitPay)	Enable digital asset payments and receive fiat currency in exchange	Provide payment-processing services to merchants and other business entities, can facilitate wallet address generation
Crypto ATMs	Standalone device or kiosk that allows public to purchase or sell digital assets at a terminal by using cash or debit	Purchase, sell or transfer digital assets for individual use

Centralized Finance	Key Characteristics	Purpose and Anticipated Activity
Non-financial Applications (examples)		
Gaming and gambling (e.g. Axie Infinity)	Video games that incorporate cryptography-based blockchain technology	Online gambling using digital assets as a payment instrument or receiving digital assets as proceeds, game-tokens may be swapped for other assets, play-to-earn proceed generation
Art / Collectables (e.g. OpenSea)	A collectible digital asset that can be tradeable in the digital world	Purchase the NFT art for personal collection or profit-making through reselling
Metaverse (e.g. Decentraland)	The virtual space that integrates the experience on trading a variety of NFTs, including real estate, art, among others and typically traded again in the secondary marketplace	Purchase game character wearables, lands and other items through Metaverse, engage in profit making by purchasing items through Metaverse and reselling
Mining (e.g. Riot Blockchain)	Entities that earn digital assets by verifying transactions on the blockchain on a PoW mechanism	Mining for the miner's own benefits and usage, property owners renting the property for crypto mining at scale, professional crypto mining company operating crypto mining at scale

Decentralized Finance	Key Characteristics	Purpose and Anticipated Activity
Decentralized Exchange (e.g. Uniswap)	Facilitate exchange of digital assets by using smart contracts	Participate in the liquidity pool by putting up their funds and receiving token contributions, automated market making for the swap or transfer of digital assets
Lending Protocol (e.g. Aave, Compound)	"Allow users to deposit collateral in the form of cryptocurrency assets and receive assets, typically dollar-denominated stablecoins, in return"	Act as the lender of the protocol to earn interests higher than what is offered by banks, or act as the borrower of the protocol to borrow digital assets for consumption or arbitrage activities
Derivatives (e.g. Synthetix)	Allow users to create synthetic assets on blockchain platforms that track the value of off-chain / "real-world" assets, as well as other on-chain assets	Purchase and sale of derivatives using digital assets very much like traditional exchange activity
Asset Management (e.g. Lido)	• Assist investors by combining their tokens into pools using smart contracts, often for use on other dapps • These pools capture traditional exposure, synthetic structured tokens, or interest-bearing accounts	Invest digital assets to tokenized pooled portfolio of digital assets. invest digital assets to aggregators, which interact with other lending protocols to identify profitable lending services

Insurance (e.g. Nexus)	Leverage the self-executing smart contracts and eliminate the needs for claims adjusters and even claims themselves	Purchase a variety of cover products and be paid out if the claim is approved by the claim assessment process
DAOs	Organizations or businesses that leverage the blockchain's smart contract technology to make shared decisions on behalf of its members	Fundraising, general governance, including voting, or participation in a social network, sell, purchase or swap of digital assets

Blockchain Tools & Service Providers	Key Characteristics	Purpose and Anticipated Activity
Mixer and Tumbler	Services which co-mingle funds from different users, making it challenging to trace funds to their ultimate source	Conceal the identity of the users and the details of the transactions so deposits and withdrawals are difficult to match
Cross-chain Bridges (e.g. cBridge)	• A type of virtual service that allows users to exchange tokens on one blockchain to another • Both centralized bridge (e.g., Binance Bridge) and decentralized bridge exist	Chain hopping to facilitate compatibility and interopability across different blockchains, potentially used to layer transactions and obfuscate trails
Crypto Swap [e.g. ChangeNOW, Shapeshift]	Allow users to swap cryptoassets for other tokens, either on the same or different blockchains	• Exchange cryptos more quickly and efficiently • Illicit swapping of digital assets to a variety of other digital assets or physical cash to launder money
Key Management and Service Providers (e.g. MetaMask, Ledger)	Entities involved in developing infrastructure services that would manage keys on behalf of users or enable users to manage their own keys	Provide online of offline wallet solutions to safeguard private keys

About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com