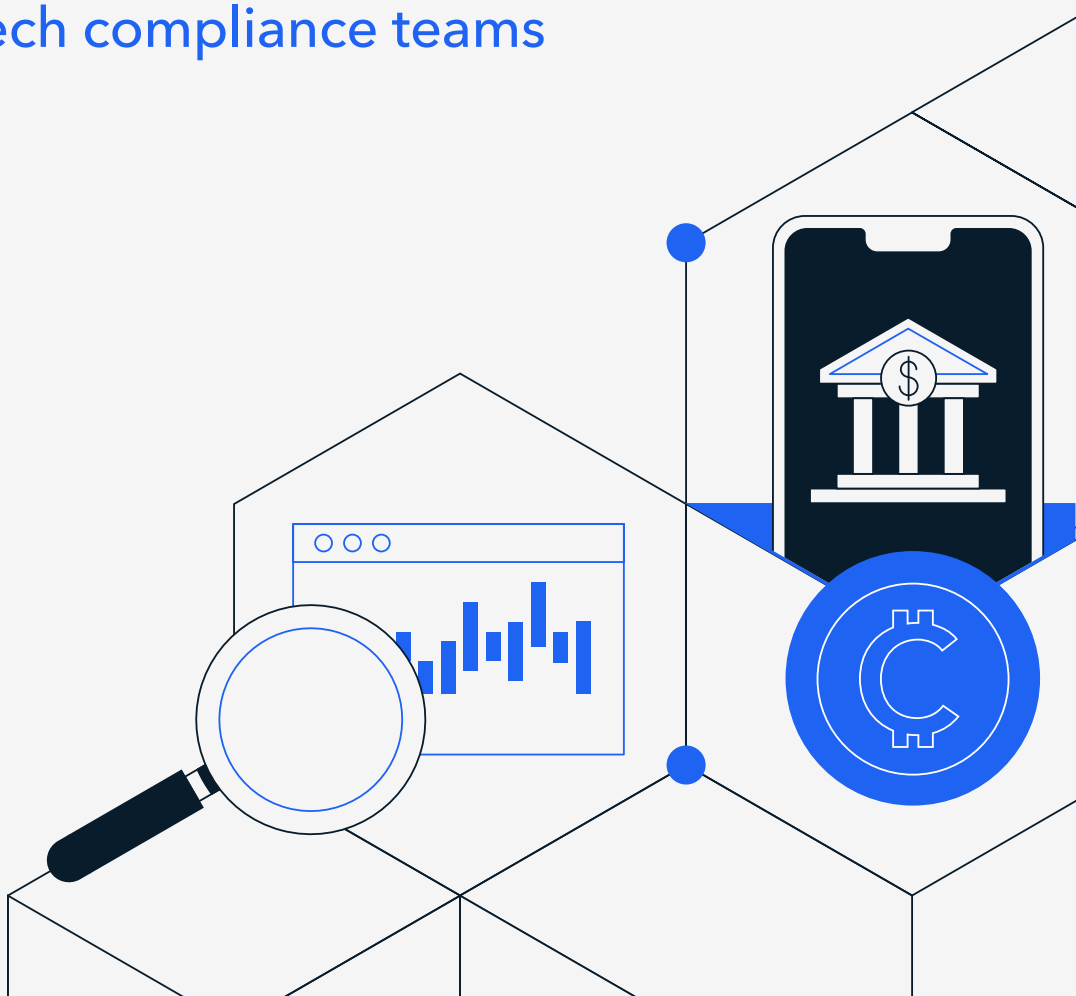
TRM WHITE PAPER

Managing Risk in the World of Crypto Payments

A guide for fintech compliance teams



TRMLABS.COM

Payment service providers: The bridge between crypto and fiat currencies

Digitization and technology have driven explosive growth and innovation in the world of payments. According to EY, payments businesses make up 25% of all fintechs, and are collectively valued at over USD 2 trillion.

This is true for the crypto economy as well. Aside from crypto exchanges, payment service providers (PSPs) are one of the largest groups of virtual asset service providers (VASPs). PSPs are intermediaries that facilitate electronic payments between various parties — and they play an important role in driving global cryptocurrency adoption. Based on TRM data, PSPs in over 60 countries process billions in crypto payments each year.

First, by processing cryptocurrency payments, PSPs enable more people and businesses to pay in cryptocurrencies, increasing their liquidity and utility. Blockchains and digital assets hold tremendous promise to reduce payment and settlement cost and inefficiencies, particularly across borders. At present, cross-border payments can often take days to settle, while blockchains are available 24/7 by default. And, according to Schroders, stablecoin transaction fees stand at less than 0.1%, a fraction of the 3–6% typically charged for cross-border retail payments.

Second, by providing on- and off-ramps for crypto businesses to accept and pay out fiat currencies, PSPs act as a bridge for value transfer between the crypto and fiat ecosystems. With trillions in value circulating in fiat currencies, on- and off-ramps are critical in integrating the crypto economy with the wider financial ecosystem.

While PSPs can help deliver on crypto payments' tremendous potential and promise for consumers and businesses — value transfer at the speed of the internet — they also face unique risks by sitting at the intersection of payments and crypto.

The risks for PSPs can be diverse and complex

"Crypto exchanges have one main activity: trading. In payments, the use cases are more varied – especially in a B2B context. They range from payments for goods and services, to internal treasury, and on- and off-ramping fiat for crypto trading," explained Aaron Chua, regional head of compliance at StraitsX (a Singapore-headquartered digital asset PSP and stablecoin issuer) and former compliance director at a crypto exchange. "Knowing the use case is key to managing risk effectively."

"What constitutes suspicious behavior depends on the client's use case. You need to know what they are using the account for, who their vendors and customers are, and the profile of the business," added Chua. For example, high-value, low-volume transfers occurring at fixed intervals could be business as usual for a corporate treasury account, but look out of place in a B2C merchant account.

In the customer due diligence process, PSPs also need to have a precise methodology for identifying truly high-risk customers. Providers that classify entire categories of businesses as "high-risk" are not consistent with risk-based approaches and often lack appropriate enhanced due diligence triggers. Moreover, they could miss out on opportunities with legitimate customers by taking an overly conservative approach to risk.

> *"What constitutes suspicious behavior depends on the client's use case. You need to know what they are using the account for, who their vendors and customers are, and the profile of the business."*
>
> Aaron Chua
> Regional Head of Compliance, StraitsX

For example, following the outbreak of the Hamas-Israel conflict, there was significant discussion on the use of crowdfunding platforms by terrorist groups. However, this does not make every crowdfunding platform a high-risk customer. In its "Crowdfunding for Terrorism Financing" report, the Financial Action Task Force (FATF) noted that "[c]rowdfunding is a very useful way to reach a large audience" and that "the vast majority of crowdfunding activity is legitimate."

Nesting helps PSPs expand reach, but also presents regulatory risk

Another key risk for PSPs comes from nesting arrangements.

Nesting – where a PSP uses the rails of another PSP to provide services to their customer – can be a legitimate business arrangement to reduce cost, expand reach, and increase economies of scale. It is a well-established practice that is not unique to PSPs. Correspondent banking – where one bank provides services on behalf of another (usually foreign) bank – is a form of nesting, and has been around for centuries.

> *"Although nesting can occur in the context of any financial service, some features of the Payment Sector – the long payment chains and the involvement of multiple parties – can increase the likelihood that nesting will take place. In particular, some Payment Sector participants specialize in providing financial services to dubious merchants or customers who would be rejected by larger financial institutions."*
>
> Guidance for Licensed Financial Institutions on the Risks Relating to Payments
> Central Bank of the United Arab Emirates' Rulebook

However, unauthorized nesting, which often seeks to circumvent local laws, can expose PSPs to significant regulatory and reputational risks. For example, they could be facilitating unlicensed activity, or unwittingly providing payment services to high-risk customers. Indeed, there are PSPs that exist primarily to serve illicit actors.

Even in authorized arrangements, there are risks that need to be managed. In many cases, nesting means PSPs are processing payments for clients of clients, which naturally reduces visibility and increases risk. The PSP would be relying on the due diligence of its PSP client and may not have access to the KYC information of the end client.

"Applying multiple layers of controls, as well as constant, open communication with clients is critical in managing this risk," shared Rodrigo Peiteado, financial crime intelligence lead at BVNK, a UK-headquartered payments infrastructure provider. "You also need to be very responsive to changes in client behavior, for example if they stop being forthcoming in their communications."

Data is key for risk management

Timely and comprehensive transaction data is another key piece of the PSP risk puzzle. Here, FATF Recommendation 16 – more commonly known as the Travel Rule – has set the standard since it was introduced in 2001.

Recommendation 16 requires financial institutions to exchange a predefined set of sender (originator) and recipient (beneficiary) information for every wire transfer transaction. "This exchange of information provides an important source of data in payment transactions," said Simona Suskeviciene, director of financial crime compliance product advisory at BVNK. "It is a well-established requirement in the fiat world, which is now being applied to virtual assets via the FATF Travel Rule."

How crypto changes the paradigm

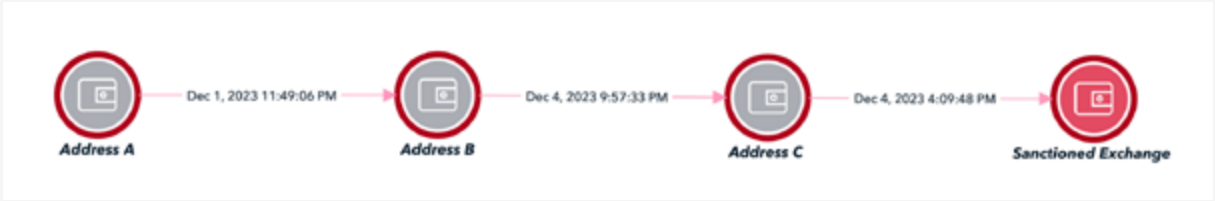
Data

When it comes to data, the transparency and traceability of blockchains give crypto an edge over fiat. "Being able to trace the flow of funds on-chain provides a new level of transparency. You are able to see suspicious activity beyond the direct counterparty, and evaluate indirect risks," Suskeviciene said.

WHAT IS INDIRECT RISK?

Indirect risk is the ability to see suspicious activity away from your customer or institution, often discussed in "hops."

For example, in the image below, Address A has two wallet addresses between it and a sanctioned exchange. Thus, Address A may have indirect sanctions risk exposure.



When examined through blockchain intelligence platforms that attribute transactions and addresses to real-world persons and entities, this data offers PSPs a wealth of information to better understand the profile of clients and counterparties. However, there are some limitations.

"In cases where wallet addresses are not associated with known actors, it can be challenging to know who the funds belong to. We still need the client and their counterparty to provide this information," explained Suskeviciene. "The Travel Rule addresses this gap, providing an additional layer of protection, though there are some implementation challenges that providers need to overcome in the coming weeks and months."

In the world of virtual assets, FATF Recommendation 16 is still in its sunrise period: a transitional phase where the Travel Rule has yet to be uniformly implemented across different jurisdictions. VASPs thus face practical difficulties in exchanging Travel Rule data.

For example, a VASP in a jurisdiction that has yet to fully implement the Travel Rule may not have the systems or information to send the required information to another VASP that is required to comply with the Travel Rule. In Notabene's 2024 State of Crypto Travel Rule Compliance Report, the VASPs surveyed identified sunrise period effects as the second greatest hurdle to Travel Rule adoption. 37% of respondents had also not received any Travel Rule requests from other VASPs.

That being said, "crypto assets definitely still have the advantage when it comes to detecting and preventing financial crime, because of the transparency of public blockchain data," Suskeviciene noted.

Speed

The lightspeed at which crypto and blockchain enables value transfer is a double edged sword for PSPs. It makes payments faster, better, and cheaper – for both legitimate and nefarious actors. This means that risk and compliance teams must act quickly to detect and disrupt illicit activity, or risk missing the opportunity altogether.

"Bad actors move very quickly on-chain,"shared Chua. "Once they convert fiat currency into stablecoins, it goes off our platform very quickly, usually into self-custodial wallets, making it more difficult to recover the funds."

The speed of blockchain technology is not just about the rapid transfer of funds from one wallet address to another with instantaneous settlement. It also relates to the speed in which new wallet addresses can be created.

This may be done for benign, operational reasons within VASPs – for example, where they may enable users to create a large number of wallet addresses with the same seed phrase to manage accounts more efficiently. Or it may be done for illegitimate reasons by illicit actors or entities looking to generate fresh, untainted addresses. Those addresses can then be leveraged to facilitate a limited set of transfers before they are discarded. Then, new addresses are created again – repeating in a continuous cycle, with the aim of making it harder for PSPs to track transactions and pinpoint risk exposure.

> *"Crypto assets definitely still have the advantage when it comes to detecting and preventing financial crime, because of the transparency of public blockchain data."*
>
> Simona Suskeviciene
> Director of Financial Crime Compliance Product Advisory, BVNK

"Unlike creating a new bank or payment account, creating a new self-custodial wallet address is a frictionless, no-KYC process. Some bad actors have even automated the process, which is why it's important for service providers to have the right AML tools and systems in place," said Peiteado.

Why a holistic approach to compliance is crucial

Given the revolving door of wallet addresses that bad actors may use, choosing a blockchain intelligence platform with robust and automated attribution expansion capabilities is paramount.

Other tools and controls can also complement on-chain surveillance. "The best time for us to stop a bad actor is before they act," said Chua. "This is why we employ a whole suite of compliance tooling to detect suspicious activity, from unusual login locations to unusual wallet behavior. But the human element is most important: there are some behaviors that, in isolation, may not be suspicious, but tell a different story when pieced together. Compliance teams need to be trained to look at the whole picture, and develop expertise to make the right judgment calls."

> *"Some bad actors have automated the process [of creating a new self-custodial wallet address], which is why it's important for service providers to have the right AML tools and systems in place."*
>
> Rodrigo Peiteado
> Financial Crime Intelligence Lead, BVNK

Compliance by design

The use of blockchain technology also opens up new possibilities for compliance by design. The Monetary Authority of Singapore's Project Orchid explored the concept of purpose-bound money (PBM), a form of programmable money where "the conditions upon which an underlying digital currency can be used" are pre-specified. PBM has been used to digitize government and commercial vouchers, and facilitate government payouts.

This programmability can be applied to compliance as well. "The basic idea of PBM is that the underlying digital monies and stablecoins can only be used for payment under certain conditions. These could include specified payees, specified transaction thresholds, and more," explains Chua. "This could allow businesses and compliance teams to specify predetermined transaction characteristics to reduce risks and even embed certain due diligence checks."

Staying ahead of the curve

For fintechs looking to provide faster and cheaper payments to their customers, blockchain technology holds great potential not only for innovation, but risk management. With the right expertise, tools, and culture, businesses can leverage the transparency, traceability, and immutability of public blockchains to detect and prevent financial crime in new ways.

For more insights, download our crypto compliance whitepaper here.

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