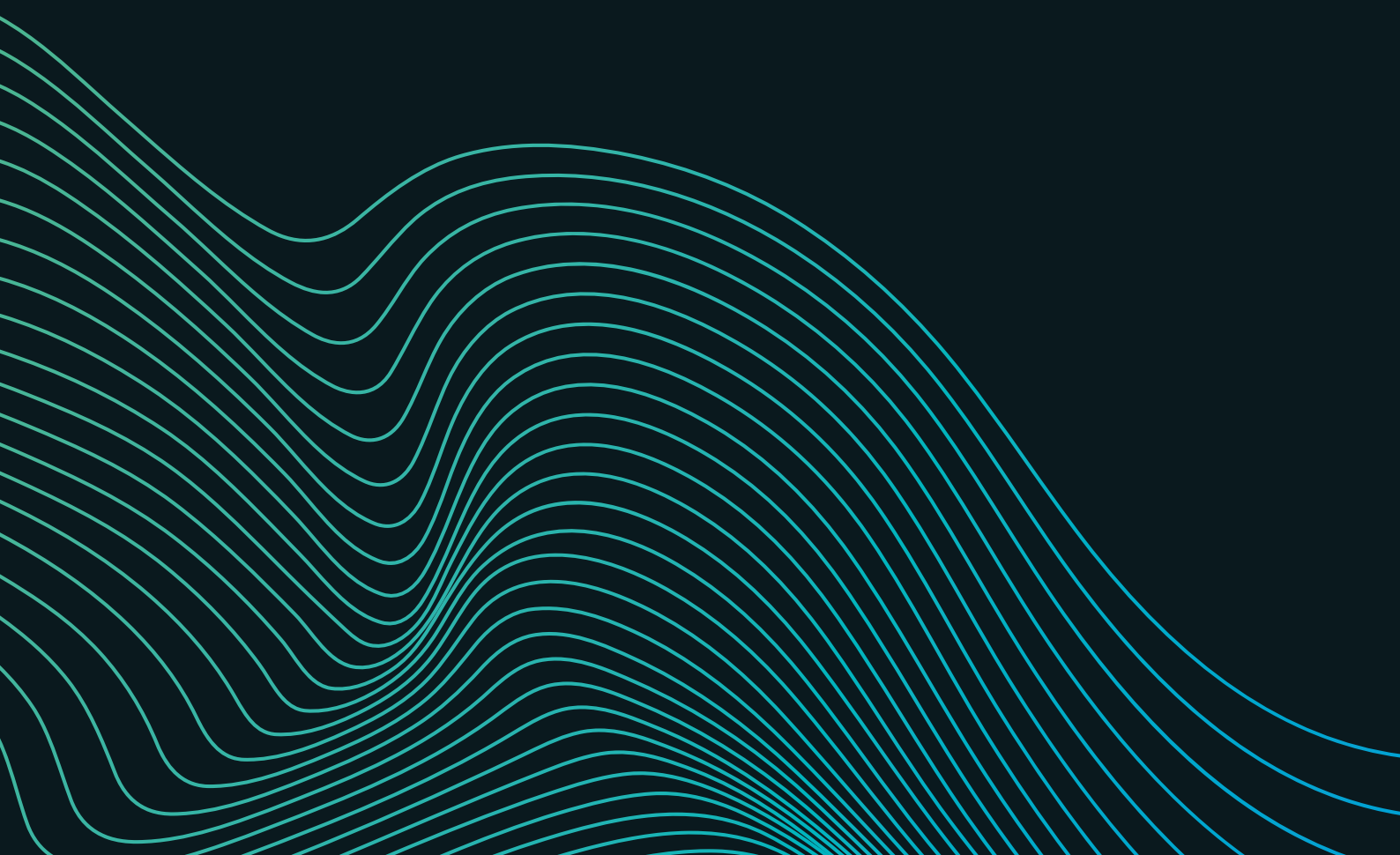
PLENITUDE

Crypto compliance solutions and their place in a risk management framework



It is increasingly clear that the blockchains on which bitcoin and other cryptoassets transactions are recorded are a valuable forensic tool that is being used more widely by law enforcement and the intelligence community to identify and disrupt illicit activities. This also opens up opportunities for traditional finance (TradFi) firms and cryptoasset providers[1] to deploy more effective preventive, investigative and forensic capabilities in order to detect, deter and prevent financial crime.

Capitalising on the intelligence that blockchains provide, an entire sector has sprung up to utilise this information, turning it into actionable data for law enforcement, regulators, compliance teams and investigators.

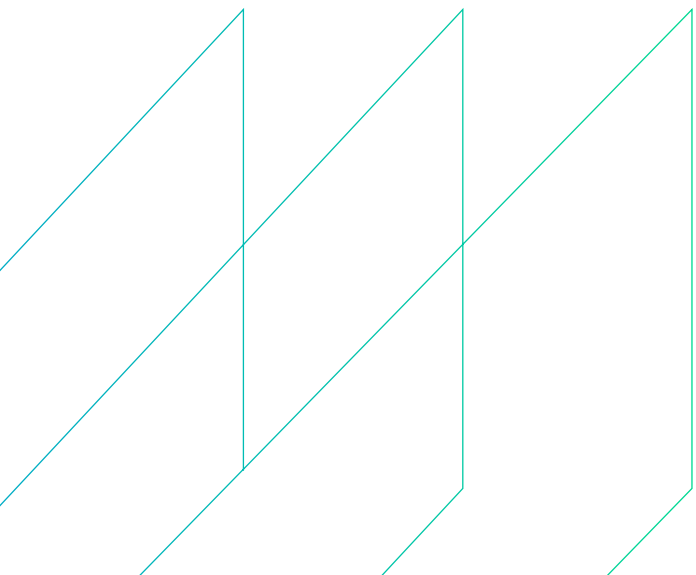
It is thanks to this data that we can estimate how much crypto activity is actually associated with crypto-native illicit activity: according to the latest Chainalysis Crypto Crime report, in 2021 this figure was around 0.15% of total transaction volume[2], continuing a consistent downwards trend from 0.62% in the previous year. This is due to industry efforts to more effectively combat illicit activity and also the significant inflows from retail and institutional actors, that have outstripped illicit flows. However, fraud and cybercrime continue to be a significant industry issue, with recent figures in the same report estimating ransomware payments in 2021 at more than USD 600 million, and stolen funds at more than USD 3bn, mostly from DeFi (decentralised finance) protocol exploits, a number that is looking to be exceeded this year, which has featured several high-profile bridge exploits amongst other security incidents.

What are they, and how do they fit in a firm's risk management framework?

Crypto compliance solutions (and in particular the compliance-focussed blockchain analytic tools that are the main object of this article) allow users to take a random series of characters (public addresses on the blockchain) and turn them into human-readable names through the clustering and labelling of addresses. This is achieved through a combination of OSINT[3], information gathered by networks of analysts and contacts in the law enforcement community, and the collective community of users of the tools. The tools also frequently make use of AI and machine learning to determine, with a high degree of certainty, whether addresses belong to an identified counterparty.

The crypto compliance solutions space is very active, with large established vendors such as Chainalysis, TRM Labs, Elliptic and more recent challengers such as Coinfirm and Scorechain amongst others. While there are some common capabilities, there are also key differences in coverage and functionality, with vendors constantly looking to improve and rapidly add new features to their solutions and tools.

One clear pattern that has emerged from the current state of crypto regulation is that regulators expect crypto firms to apply the same regulations that are applicable to TradFi firms, at least when it comes to AML/CTF and Sanctions. Most licensing and registration regimes currently in place seek to mitigate these risks by imposing a requirement for crypto firms to implement an effective AML/CTF framework with supporting systems and controls.



[1] Referred to as VASP, CASP, PSAN, etc. depending on the country

[2] This number is likely to be revised as further illicit activity is labelled, but is indicative of a downwards trend that goes back several years as the crypto industry matures and reaches more investors

[3] Open Source intelligence, for example combing internet forums, darknet marketplaces, etc. for actionable information

In practice, this means that some of the systems and controls required in TradFi firms, need to be adopted by crypto firms.

1. Appropriate oversight and governance
2. An assessment of AML/CTF and Sanctions risks
3. A risk-based approach that mitigates the risks identified from the risk assessment
4. Robust policies, standards, and procedure
5. Appropriate systems and controls for sanctions, payment screening, transaction monitoring, etc.

However, crypto presents unique risks and use cases that are not addressed by systems and tools typically used in TradFi, and this is where crypto compliance and blockchain analytic tools come in. They are unique to crypto and key to assess a number of factors, such as:

- Wallet screening, to determine the riskiness of specific addresses. This feature is very powerful when used in conjunction with investigations or forensics to track the source and destination of funds when onboarding clients or before processing withdrawal requests;
- Transaction monitoring, which allows users to customise alerts based on the interactions of clients' wallets and transaction patterns;
- Forensics, which is mostly used on a reactive basis to investigate the destination of funds following hacks, ransomware incidents, etc.;
- Identification of sanctioned counterparties, which the tools label to assess direct or indirect exposure;
- Basic information and risk scoring on VASP counterparties, to support due diligence

Key considerations when selecting a crypto compliance solution or tool:

There is no one-size-fits-all when selecting the 'right' tool, what works for one firm may not work for another. Tools differ in their coverage, capabilities and cost, so it is important that firms clearly define their requirements based on their activities, risk profile and use cases, in order to comprehensively assess the solutions that exist in the market place. Key factors to consider and evaluate are the following:

Chain Coverage

Chain coverage is a key distinguisher as it can range from about 10 chains and their tokens in some tools, to 40 and above in others, meaning more than a thousand assets in some cases. These numbers are growing fast across the board, as all vendors are conscious of the need to expand coverage as much as possible. Firms should consider how much coverage they need depending on the assets they are exposed to: for example, a smaller custodian or exchange that only deals with a limited number of coins or tokens will require less coverage than a large exchange that deals with hundreds.

Investigation Capabilities

The ability to trace the origin and destination of funds is essential. Besides, funds can now easily move from one chain to another, making cross-chain investigation capabilities an increasingly crucial differentiating factor. Although all tools allow the movement of funds to be displayed graphically and annotated, as well as graphs to be exported, they still differ widely in the type of data that accompanies certain aspects of the graphs, and the tooling available to build legible graphs. It must be noted, however, that investigation features may be more pertinent to law enforcement and regulators who are routinely involved in tracing funds' movements, and may only be occasionally needed by private sector players. On this basis, most providers allow users to choose the modules they wish to use.

Counterparty Due Diligence

This can be a useful first step to gather information about VASP counterparties and assess their risk: the best tools combine off chain and on-chain data to not only give an idea of legal entities, executives, existence of AML policies, etc., but to also analyse exposure to different counterparties and illicit activity. However, in their current state, these reports are not comprehensive to the point that due diligence can be based exclusively around them, so firms will need to complement this information with additional due diligence.

Transaction Monitoring

Transaction monitoring tools allow entities to create scenarios that fit their risk appetite and focus on the patterns of behaviour, or types of counterparties, that correspond to their business activities or identified risks. Tools differ in the number of scenarios and criteria that entities can define and adjust to generate alerts.

Risk Scoring

Existing tools differ in the methodology they use for risk scoring addresses, as well as the ability to fine-tune criteria depending on an entity's risk appetite. They also differ in the way they display these results, with some that calculate a single risk score, while others distinguish between incoming and outgoing flows, with different scores for each, and also different scores for each asset. Likewise, some tools provide the possibility to distinguish between direct and indirect exposure. The quality and level of detail of the information displayed when screening a wallet will also vary significantly from one tool to another.

Training and Support

Most interfaces are quite intuitive, but users will need training to fully exploit all available features of the tools, especially when conducting investigations or building graphs. All tools include help centres and guides with varying levels of detail, but timely access to support teams and training can greatly facilitate the onboarding of users and the speed at which they become proficient in using the tools.

Sourcing and Reliability

Information sourcing and address label reliability are mostly dependent on the strength of the network of analysts and third parties contributing to the clustering and labelling of address, as well as the quality of AI / machine learning algorithms. Approaches can be probabilistic or deterministic and may result in more or less false positives depending on the strength of these. Firms should probe vendors on the quality of the input data and figures on the prevalence of false positives, and reliability of labelling.

Pricing

Pricing varies widely from one tool to another and is determined by the services a firm is subscribing to, the number of licenses, length of contract, need for APIs, etc. Firms with different levels of exposure and activity will have different needs, which will require different levels of investment.

Conclusion

It is evident that crypto compliance solutions are essential in the industry's efforts to more effectively combat illicit activity and financial crime. As crypto adoption increases, more players seek to enter the industry and the regulatory framework evolves, incumbent firms and new entrants will be required to upgrade or deploy new crypto compliance solutions.

The number of crypto compliance solution vendors in the marketplace continues to increase at pace with over a dozen players, which presents a challenge to firms when seeking to select a vendor. Therefore, firms need to fully understand the risks they are seeking to mitigate and comprehensively define their requirements and use cases, in order to effectively assess the multitude of crypto compliance solutions that exist. This can take significant time and effort, and if the wrong solution is selected, can result in wasted investment or a solution that does not fully address the risks or requirements of the firm.

Plenitude has a deep understanding of the crypto compliance solutions that exist in the marketplace and has recently completed a comprehensive assessment of multiple vendors. We are able to assist firms in the selection and implementation of a crypto compliance solution that best meets their requirements, mitigating the risks associated with selecting a vendor.

ABOUT PLENITUDE

Plenitude is a niche consultancy, specialising in Financial Crime Risk and Compliance, and are appointed to the Financial Conduct Authority's Skilled Persons panel for Financial Crime. Our focus is firmly on addressing the legal, regulatory, reputational and social imperative for financial institutions to take diligent and rigorous steps to mitigate financial crime risks.

Plenitude's Digital Assets offering aims to accompany Financial Institutions that wish to understand the crypto industry and its associated risks better, with a view to gaining a better grasp of this fast-evolving sector and adapt their strategies to best take opportunity of emerging opportunities in this area. This ranges from developing crypto trading and awareness activities to assessing financial crime risks associated with crypto business models, developing, and implementing policies and procedures, and providing guidance on crypto compliance solutions and assisting with selection and implementation.

About the author

Manuel Fajardo is our Digital Assets Practice Lead, with over 17 years of experience in the global asset management industry across control functions like Compliance, Internal Control and Internal Audit, in positions with a global remit based in Paris, London and Los Angeles.

Prior to working with Plenitude, Manuel built the global compliance framework for a major investment management group. This involved designing, deploying and constantly refining processes, tools, policies and procedures. His main areas of focus are Anti-Money Laundering, International Sanctions and Financial Promotions / Distribution, in which he has proved adept at balancing local and global considerations and regulatory constraints, the interest of all stakeholders and firms' risk appetite to build solid frameworks that have proved successful throughout the years.

Manuel has a deep knowledge of the cryptoassets industry, acquired through more than six years of studying, investment and advisory work. In the current phase of his career, he has used this knowledge to train companies in the traditional finance sector about the significance of this nascent industry and its developing regulatory framework, as well as advising crypto firms on their regulatory obligations as they seek registrations or conduct business as regulated firms, and playing an active role in shaping discussions on regulation through industry trade bodies.

PLENITUDE

PLENITUDECONSULTING.COM

FOR MORE INFORMATION EMAIL US AT
MANUEL.FAJARDO@PLENITUDECONSULTING.COM