BASEL INSTITUTE ON GOVERNANCE

EUROPOL

Seizing the opportunity: 5 recommendations for crypto assets-related crime and money laundering

2022 Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies

Public information

As the use of crypto assets expands into practically every country and sector, so does its abuse to commit new forms of crime and launder criminal proceeds. Yet with the right tools, capacity and cooperation, the unique characteristics of blockchain-based technologies offer an unprecedented opportunity to investigate organised crime and money laundering networks and to recover stolen funds.

These recommendations follow the 6th Global Conference on Criminal Finances and Cryptocurrencies on 1–2 September 2022. The conference was hosted by Europol at its headquarters in The Hague, the Netherlands, with the support of the Basel Institute on Governance through the joint Working Group on Criminal Finances and Cryptocurrencies.

The Recommendations are intended to highlight broad approaches and best practices. They are designed to help public and private actors stay one step ahead of those seeking to abuse crypto assets (also known as virtual assets) and services to make, hide and launder illicit money.

1. Break down silos between "traditional" and "crypto"

The separation between "traditional" and "crypto" organised crime and money laundering is increasingly unhelpful. Specialised crypto expertise remains essential for both law enforcement and AML compliance teams in the private sector. This is in part due to the highly technical nature and fast evolution of blockchain-based technologies. But recent trends in criminal activity and the use of cryptocurrencies to launder money show how the two worlds are merging. Efforts to combat such crimes in both the public and private sectors need to do the same.

As cryptocurrencies and other crypto assets start to merge with mainstream financial markets and services, so too do organised crime and money laundering involving crypto assets. The line between physical and virtual is blurring fast.

- **Crypto assets are increasingly involved in traditional money laundering typologies** like trade-based money laundering, and linked to a broad range of crimes from drug smuggling to sports match fixingor fraud.
- **Professional money launderers are taking advantage of the ever-growing options provided by crypto assets** to launder proceeds from both online and offline crimes.
- **Criminal synergies are growing between the physical and virtual spaces:** perpetrators of online scams use money laundering services provided by traditional criminal networks, for example.

Yet in regulations, policies, law enforcement approaches and in the private sector, "crypto" organised crime and money laundering is all too often treated as a separate area that can only be investigated by special cybercrime units. However, those specialised units are not the ones involved on the ground and they are not involved in all cases. This **overlooks opportunities to detect, investigate and prosecute** crimes and money laundering that span both the physical and virtual domains.

Specialised expertise will remain essential, due in part to the highly technical nature of crypto assets and the fast evolution of the industry. But to break down silos, more could be done to **build basic blockchain/crypto training into onboarding and ongoing professional development.** This would be valuable for all law enforcement agencies and other relevant public authorities, including financial intelligence units, judicial authorities and regulatory/supervisory bodies in relevant sectors.

Financial institutions and other entities with AML/CFT obligations should also consider introducing blockchain/crypto training for relevant staff, considering their position in the **front line of detecting and reporting suspicious transactions**.

Within both law enforcement and the private sector, **multidisciplinary teams** can bring together specialists from financial crime, organised crime, crypto and cyber units to cooperate on cases and share knowledge. This can help bridge the divide between different areas of expertise and practice, without impacting significantly on resources.

2. Regulate broadly and make full use of existing laws

Existing financial crime laws can be (and are being) applied to prosecute crimes and money laundering involving crypto assets and to recover illicit funds. Legislators can make it easier for law enforcement, prosecutors and judges to deal with cases involving crypto assets by considering these when developing new financial crime laws or revising existing legislation. It is essential that crypto assets are treated like any other asset for the purposes of AML/CFT supervision and enforcement.

The merging of crypto assets into traditional financial markets and services makes it vital for legislation to bring crypto assets (and service providers) into existing AML/CFT frameworks. Upcoming European Union regulations on markets in crypto assets and transfer of funds, for example, seek to do just this, as well as to harmonise rules across the region to prevent criminals from moving to jurisdictions with weak laws and oversight.

Legislation is by nature slow to develop and even slower to come into force. But decades-old laws on money laundering, wire fraud or other relevant areas can be (and have been) used to prosecute criminals that abuse crypto assets to commit crimes or launder money. **Existing asset recovery laws, both**

conviction and non-conviction based, have enabled some jurisdictions to confiscate large amounts of illicit crypto assets.

When developing new financial crime legislation or revising existing laws, such **laws should be broad enough to cover crypto assets** and capable to anticipate future evolutions in the crypto industry. This will make it easier for law enforcement, prosecutors and judges to apply them to all cases, whatever the nature of the asset involved. **Public consultations** can help ensure new or revised laws are fit for purpose in this fast-evolving industry.

3. Take advantage of the blockchain to disrupt organised crime

The blockchain technology that forms the backbone of crypto assets and services offers numerous opportunities to investigate crime and money laundering schemes, gather intelligence, and freeze and confiscate illicit assets.

Despite talk of the "threats" of crypto assets and services, these pose no more of an inherent threat than cash, companies, property or even the global trading system – all of which are still far more likely to be used to launder illicit funds. Latest estimates indicate that the **percentage of illicit activity in the crypto industry is decreasing**, even as the use of cryptocurrencies expands and evolves.

What the blockchain does offer is promising **opportunities to investigate and disrupt organised crime networks and to recover illicit assets.** With the right tools, techniques and data, law enforcement can (and does in many countries) "follow" illicit assets as they move across one or more blockchains. This presents opportunities to:

- I**dentify the individuals** behind the scheme – often because criminals themselves make mistakes that reveal their identity.
- **Broaden investigations** to other individuals or companies, potentially revealing new leads and uncovering wider organised crime networks.
- **Generate intelligence** on how the crypto assets are being laundered, enabling the development of smarter strategies and tactics.
- **Gather evidence of illicit activity** for use in court that, due to the nature of the blockchain, cannot be destroyed and can be seen and interrogated by all.
- **Confiscate illicit assets**, even if the individuals behind the scheme cannot be identified or are hiding in a jurisdiction from which they cannot be extradited.

4. Raise crypto literacy through capacity building and clear communication

Increasing general understanding of crypto assets and services is vital to tackle organised crime and money laundering, both physical and virtual. Finding smart ways to communicate about crypto also pays off.

The technical language and acronyms that have evolved around the crypto assets industry are a major barrier to addressing crypto-related crime and money laundering.

Ordinary users need to understand the risks of investing in crypto assets to avoid scams and theft. Law enforcement officers need to understand their counterparts when they present a case study of a crypto-related money laundering scheme. International cooperation between law enforcement will go nowhere if counterparts across borders don't understand what is being requested. And prosecutors need smart ways to explain clearly to judges how money was laundered through the crypto sphere to increase their changes of a successful conviction.

It is recommended that:

- Law enforcement officers even in low-resource countries can make use of **free courses and resources available online**. This will help them to broaden their knowledge and become familiar with the terminology around crypto assets and the different ways of storing them.
- **Standard operating procedures** are developed (either at the national or international level) that describe what needs to be done to preserve digital evidence, how to locate crypto assets, and the correct way to secure them once they are seized.
- When describing a case, prosecutors should make ample use of **graphs and visualisation tools** to illustrate the flow of money through wallets and addresses.
- More **events, seminars and workshops** will help law enforcement and other stakeholders to share and acquire knowledge.

5. Increase public-private cooperation

Public entities, including law enforcement bodies, can gain significantly by harnessing the tools, data and analytics expertise of the private sector. Closer cooperation with crypto asset service providers can also speed up law enforcement requests to assist investigations and freeze funds.

There are little sectors that benefits more from public-private cooperation than crypto, and in several ways.

One way concerns **investigative tools and capacity**. Private blockchain analysis and asset tracing companies are innovating fast. Many already have high-powered tools and analytical capacity to trace funds laundered across multiple blockchains using different obfuscation techniques. Developing such tools and capacity in-house is not feasible for most law enforcement bodies. Similarly, asset management is another area in which the private sector can play an important role.

In addition, specialised blockchain companies can often draw **valuable insights** into crypto-related money laundering typologies from the vast amounts of data they hold and analyse. Sharing such findings with law enforcement can help to trigger investigations and inform more targeted strategies. This could be done via new or established platforms and channels for information sharing.

Speed and efficiency would also increase greatly with closer public-private cooperation. Transactions involving crypto assets take place extremely fast. Money laundering schemes can often involve multiple blockchains and mixers located in different jurisdictions, making it more difficult for law enforcement to follow the money. The nature of crypto assets therefore demands a high-speed reaction from law enforcement. This is especially true when a case spans multiple jurisdictions.

Traditional cross-border procedures, such as European Investigation Orders, freezing orders and mutual legal assistance requests, will never be fast enough to obtain information or evidence or even to freeze suspect crypto assets before they are transferred. Closer cooperation with crypto asset service providers, in particular when these operate dedicated departments for liaison with law enforcement, can help to speed up the execution of requests for information and for precautionary freezing of suspect funds.