






A race against time: Europol – Basel Institute on Governance recommendations on preventing and combating the criminal use of cryptocurrencies

These recommendations follow the 7th Global Conference on Criminal Finances and Cryptocurrencies on 26–27 October 2023. The conference was co-organised by Europol and the Basel Institute on Governance and took place in hybrid format at Europol's headquarters in The Hague, Netherlands.

The Recommendations highlight broad approaches and best practices to prevent and combat the use of crypto assets and services to make, hide and launder illicit money.*

Recommendations

-  **1** Accelerate innovation for investigative and monitoring tools
-  **2** Boost enforcement capacity and training
-  **3** Reorganise to foster collaboration and prioritisation
-  **4** Engage proactively in multi-sector collaborations
-  **5** Consider the whole chain, from prevention to facilitators

* This paper uses “crypto assets”, “cryptocurrencies” and “virtual assets” broadly to refer to any blockchain-based technology used to transfer and store value.



1. Accelerate innovation for investigative and monitoring tools

Serious investment in the development of new investigative and monitoring tools is needed to keep up with the criminals.

Blockchain-based technologies and applications are evolving fast, boosted by other technologies such as artificial intelligence or AI. **How they are used and misused also evolves fast.**

As a result, **investigators face increasing challenges in tracing illicit crypto assets.** Law enforcement is increasingly able to trace, locate and dismantle centralised services used for illegal activities as well as mixers that “mix” tainted and legitimate cryptocurrency for money laundering purposes. But new forms of decentralised finance and “unstoppable” smart contracts – self-executing pieces of code with the terms of the agreement directly written into code – are more of a hurdle.

Criminals also exploit the thousands of different cryptocurrencies, blockchains and crypto-ecosystems now available, as well as the power of AI. They use swaps and bridges, hopping from one blockchain to another, to obfuscate the final destination of the profits of illegal activities.

Law enforcement must do more to keep up with both technological developments and the evolution of criminal tactics, from new scam and money laundering typologies to the use of cryptocurrencies that are untraceable using current tools. That will require rapid innovation, including experimenting with AI to, for example:

- Untangle complex transactions on and across blockchains.
- Identify suspicious patterns of activity or anomalies.
- Aid real-time transaction monitoring.

To take just one example, with access to mempools – the “waiting rooms” of blockchains where pending transactions are stored – AI-powered software could potentially detect suspicious transaction patterns even before this information is recorded on the blockchain.

Realising this innovation will need serious investment, from governments as well as private investors.

But there are clear benefits. Governments will gain significantly by reducing the amount of illicit funds channelled through crypto assets. Private firms can make their compliance and monitoring more efficient and effective. And there is good news: masses of publicly available data already exist to train AI tools. Crypto transactions are transparently recorded on blockchains and visible instantly, globally, to anyone – unlike transactions made in cash or between banks, for example.

The development of high-tech tools capable of tackling high-tech crimes will require close collaboration between law enforcement and technology firms, virtual asset service providers, academia and others, plus clear and transparent governance principles.



2. Boost enforcement capacity and training

Broad and strategic training is needed to ensure new FinTech is properly policed.

Cryptocurrencies are now used across **all forms of organised crime, money laundering schemes and sanctions evasion**. This is a step change from the past, when illicit funds held in cryptocurrencies tended to originate from crypto-related scams or hacks.

That means at least **a basic understanding of the crypto sphere is essential** for practically all law enforcement officers and the judiciary, as well as for financial crime compliance professionals and regulators.

A tiered training strategy, from basic to advanced levels, can optimise resources and ensure both widespread understanding among front-line officers and the development of advanced multidisciplinary units. Advanced units can not only tackle the most complex cases, but can also play a valuable role in overseeing training and knowledge transfer to a broader set of colleagues.

Whatever the level, it is crucial that training is practical and hands on, ideally involving the actual tracing of crypto transactions.

Scaling up capacity building requires strategic, long-term planning and resource allocation from a country's highest authorities, as well as the leadership of financial institutions and policy bodies.

The incentive? Investing in capacity could pay off many times over. Countries with advanced capabilities are already recovering significant quantities of assets that could potentially be reinvested in crime prevention and enforcement, as well as to return funds to the lawful owner and compensate victims or the State. And the capacity to trace crypto assets – like any financial investigation – only brings benefits in the form of better evidence, efficiency and ultimately justice.

Another incentive: if governments wish to grow their FinTech and crypto sectors, a high level of enforcement capacity is essential for investor trust.



3. Reorganise to foster collaboration and prioritisation

Law enforcement structures may need adjustment to better manage growing numbers of crypto-related cases.

The fast growth and complexity of crypto-related cases should prompt a **re-evaluation of organisational structures within law enforcement agencies**. Are these best set up to foster prioritisation and collaboration in order to maximise both efficiency and results?

For effective handling, crypto cases need:

→ **Prioritisation:** To manage increases in crypto case volumes, strategic decisions on prioritisation are essential. Some agencies have introduced systems to conduct a preliminary analysis of crypto-related cases (by humans or by machines) before high-priority cases are escalated to specialists.

→ **Collaboration *within* agencies:** Crypto investigations typically need a wide range of specialist expertise including technical, analytical, financial, open-source intelligence, cyber and others. Multi-disciplinary task forces are the key to such collaborative investigations. Crypto specialists should be included by default in law enforcement agencies' asset recovery and organised crime task forces.

→ **Collaboration *among* national agencies:** Investigations often span different agencies' responsibilities. For example, financial intelligence units need to provide investigating agencies with clear and usable information, based on the analysis of data from virtual asset service providers. Investigators and prosecutors may need the assistance of asset recovery agencies to ensure that the electronic evidence they gather is admissible in court, such as the way they have accessed cryptocurrency private keys.

→ **Collaboration *with international counterparts:*** Given crypto's borderless nature, hubs like Europol play a vital role in coordinating investigations among different jurisdictions. Greater international collaboration in the crypto sphere might also facilitate more spontaneous transmission of information between jurisdictions about potential crypto-related crime and money laundering cases. This is aided by the public and global nature of blockchain technologies, which allows more advanced jurisdictions to spot and alert their international counterparts to potential illicit activity.

Such collaborations offer a range of benefits, both for specific cases and for broader knowledge sharing.

They also support the rapid development of innovative investigative and monitoring tools (see Recommendation 1) as well as the use and adaptation of special investigative techniques to the crypto sphere. For example, techniques such as undercover agents or controlled delivery have proven to be highly effective in combating organised crime, including money laundering. Use of those techniques and their continuous refinement for crypto-related investigations is key to increasing efficiency and getting results.



4. Engage proactively in multi-sector collaborations

Private blockchain analysis firms, virtual asset service providers, academics and the tech community can all play a valuable and complementary role in tackling the criminal use of crypto assets.

Public-private collaboration is pivotal for effective enforcement against crypto-related crimes – and for those that proactively engage, such collaborations already work well. Key areas include:

- **Investigations of specific cases.** Blockchain analysis firms can provide tools and services to help investigators trace transactions and de-anonymise users.
- **Rapid responses to law enforcement requests.** Virtual asset service providers can assist investigations by providing data and swiftly freezing accounts and/or stopping transactions in response to law enforcement requests. Some take fast preliminary actions in response to urgent requests while official court orders or mutual legal assistance requests are being processed. This speed is critical given the fast nature of cryptocurrency transactions.
- **Asset management.** Seizure and confiscation require the transfer of crypto assets from an account under the control of the suspects or criminals to one which is under the control of the national authorities, and/or the transformation of crypto into fiat currency. But even a transfer can pose serious risks: a badly written transaction can render funds unusable and unretrievable forever, or allow their theft. If law enforcement agencies do not have the skills and resources needed to effectively manage crypto assets, they can seek the assistance of private asset management service providers.

→ **Strategic intelligence** on crypto-related trends and tactics. Partnerships between the public and private sectors can produce highly valuable strategic and tactical intelligence. Europol, by means of the [European Financial Intelligence Public Private Partnership](#), is a good example in this regard.

Trust is the foundation of any public-private collaboration. For example, creating and nurturing trust between investigators and virtual asset service providers allows them to communicate rapidly, providing the required information for both sides. This is important when time is of the essence. Trust is also vital for the sharing of intelligence.

Both virtual asset service providers and law enforcement could potentially also gain by engaging more with **tech or white hat/ethical hacker communities to identify vulnerabilities or gain leads after a high-profile hacks and scams.** Joining blogs, forums or even the metaverse could help investigators to understand better how the crypto world works and gather intelligence.

Collaborating with universities could also be beneficial in terms of improving research and analysis of crypto-related crime and money laundering and potentially the development of open-source tools.



5. Consider the whole chain, from prevention to facilitators

Are we doing enough to raise awareness of crypto scams – and to shut down enablers of money laundering schemes like underground bankers?

Crypto-related scams, frauds and false investment schemes continue to cause misery to victims. **Investing in awareness campaigns and education** would help protect users, improve the sector's reputation and reduce the amount of illicit cryptocurrency in circulation.

New regulations like the EU's Markets in Crypto-Assets Regulation and South Korea's new Virtual Asset User Protection Act will help prevent crypto-related crimes by, among other things, requiring **greater customer due diligence and more transparent information** for investors. These will support both prevention and enforcement efforts.

To boost prevention or at least early detection, governments could consider a **reporting system** for individuals to raise the alert about potentially illicit activity involving cryptocurrencies. Reward schemes could incentivise reporting, similar to the U.S. [whistleblowing systems](#).

Further down the chain, it is essential to look not only at criminals or money launderers but at **professional brokers, facilitators and so-called underground bankers**. Underground banking networks act as a hub for criminal cash from different areas, helping to convert cash into crypto and vice versa and to finance organised crime on a global scale. Targeting financial investigations towards assets handled by underground bankers – as Europol’s Operational Taskforces TOKEN and Backing are doing – will likely lead to significant outcomes.

Similarly, physical, unregulated **over-the-counter brokers and crypto ATMs** demand more attention. As requirements on virtual asset service providers become stricter, criminals can exploit these to break the connection between tainted cash and apparently legitimate cryptocurrency.