Crypto-assets and decentralised finance

Impact on money laundering and terrorist financing investigations led by Financial Intelligence Units

Co-funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe

Crypto-assets and decentralised finance

Impact on money laundering and terrorist financing investigations led by Financial Intelligence Units

This publication was developed within the framework of the project on the "Development of French Financial Intelligence Unit's expertise focused on digital finance and virtual assets", co- funded by the European Union via the Technical Support Instrument, and implemented by the Council of Europe, in co-operation with the European Commission. The opinions expressed in this work are the responsibility of the author(s) and do not necessarily reflect the official policy of the Council of Europe.

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Photos: Shutterstock and Council of Europe

Council of Europe Publications
F-67075 Strasbourg Cedex
www.coe.int

Printed at the Council of Europe

For more information on the subject of the publication, please contact:
Economic Crime and Cooperation Division
Economic Crime and Corruption Department
Directorate General Human Rights and Rule of Law
Council of EuropeEmail: contact.econcrime@coe.int

Authors:
Guillaume LAMBOY
Edouard KLEIN

www.coe.int/econcrime

Table of contents

Foreword

The publication of *Bitcoin: A Peer-to-Peer Electronic Cash System* by the enigmatic Satoshi Nakamoto in November 2008 is widely regarded as the starting point of the crypto-asset phenomenon. The term *crypto-asset* itself is telling — it reflects the fact that Bitcoin, and the many digital currencies that followed, are now primarily seen and used by the public as financial assets.

Yet, if we go back to that seminal white paper, Bitcoin was initially conceived as an alternative to the centralised financial systems that have traditionally underpinned much of the work of financial intelligence units (FIUs). And indeed, its technological features do potentially enable such a use. But beyond its theoretical promise, what we now face is a technology that, through its rapid democratisation, provides anyone and everyone with a tool that can fundamentally challenge the work not only of FIUs, but also of supervisors and law enforcement agencies. As a result, crypto-assets represent a new and growing risk in terms of money laundering and terrorist financing (ML/TF).

Do you know how many times the words *country or border* appear in the Bitcoin white paper? Not once. By its very nature, this is a transnational issue — which is precisely why Tracfin sought the support of the Council of Europe and the European Commission through a technical support instrument.

Together, we were able to implement an ambitious training programme: all 200 of our staff were introduced to the topic, 130 received intermediate training focused on ML/TF vulnerabilities, and 30 underwent advanced training that enabled them to engage directly with crypto-assets — not only as tools for obfuscation, but also as objects of investigation, leveraging available tools to counter such misuse. Indeed, while the intrinsic technology of crypto-assets presents certain risks, it also offers unique opportunities for the work of FIUs.

We have drawn many lessons from this constant tension between risks and opportunities. The booklet you are holding summarises some of these insights, which we are proud to share with you today. If there is one key takeaway, it is this: sharing knowledge makes us collectively stronger—when it comes to crypto-assets, and beyond.

Antoine MAGNANT

Director Tracfin

The recent period marked by the rise of crypto-assets and decentralised finance has led to a multitude of challenges in the fight against money laundering and terrorist financing. It was in this context that Tracfin requested with the European Commission a project under the Technical Support Instrument, implemented here in partnership with the Council of Europe, with a twofold challenge: first, to develop a pioneering training programme tailored to Tracfin agents and their specific needs, aimed at strengthening their skills in the face of money laundering and terrorist financing risks arising from the increasing use of crypto assets and decentralised finance; secondly, and equally importantly, share the lessons of this project with all the European Financial Intelligence Units and partners. It is in this cooperative approach that this brochure was developed as part of this initiative and in order to maximise its impact.

The European Commission is proud to support Tracfin in this process of increasing and sharing competences, an approach fully in line with other projects supported by the Technical Support Instrument – and in particular the flagship EU Supervisory Digital Finance Academy project, supporting digital finance supervisors in the 27 Member States, with the same joint objective: supporting and maintaining a community of competent authorities in a context of technological innovation, facilitating the adoption of advanced technologies and the effective implementation of the European Union's digital finance regulatory framework, also allowing for an exchange of practices between the various sectoral authorities and across borders.

Judit ROZSA

Director responsible
for the Technical Support Instrument,
SG REFORM
European Commission

In a context of rapid evolution of the crypto-asset ecosystem – reshaping global financial dynamics and creating new challenges for the rule of law – it is essential to develop a solid understanding of emerging technologies, their legitimate use as well as their potential misuse, and the most appropriate strategic and operational responses. These developments demand informed, coordinated, and forward-looking responses from policymakers, financial intelligence units, law enforcement authorities, and regulatory bodies alike.

This booklet aims to provide a concise, yet accessible overview of key concepts underpinning decentralised finance and digital assets. It explores the distinctive characteristics of these technologies, while addressing money laundering and terrorism financing risks, regulatory challenges, emerging criminal typologies, and the analytical and investigative tools available to financial intelligence units.

This work reflects the Council of Europe's long-standing work to strengthening the rule of law and addressing related threats, through institutional development and international cooperation in the fight against economic crime. The Council of Europe has long been at the forefront of addressing challenges in this area, particularly in the areas of anti-money laundering and counter-terrorist financing. It continues to support member states in building or strengthening institutional capacities to respond to emerging threats. By supporting national authorities, this publication contributes to the development of effective, coordinated, and sustainable responses to address financial risks linked with new technologies, with a particular focus on the needs and capabilities of financial intelligence units.

This publication is an initiative undertaken by the Council of Europe within the framework of the project "Development of French Financial Intelligence Unit's expertise focused on digital finance and virtual assets" co-funded by the European Union via the Technical Support Instrument, and implemented by the Council of Europe, in cooperation with the European Commission.

We extend our thanks to our institutional partners for their trust and cooperation, as well as to the authors for their valuable expertise. Through enhanced understanding and greater cooperation, we can strengthen the resilience of states' financial systems and uphold the rule of law in a rapidly changing digital era.

Gianluca ESPOSITO

Director General of Human Rights
and Rule of Law
Council of Europe

Crypto-assets, money laundering and terrorist financing

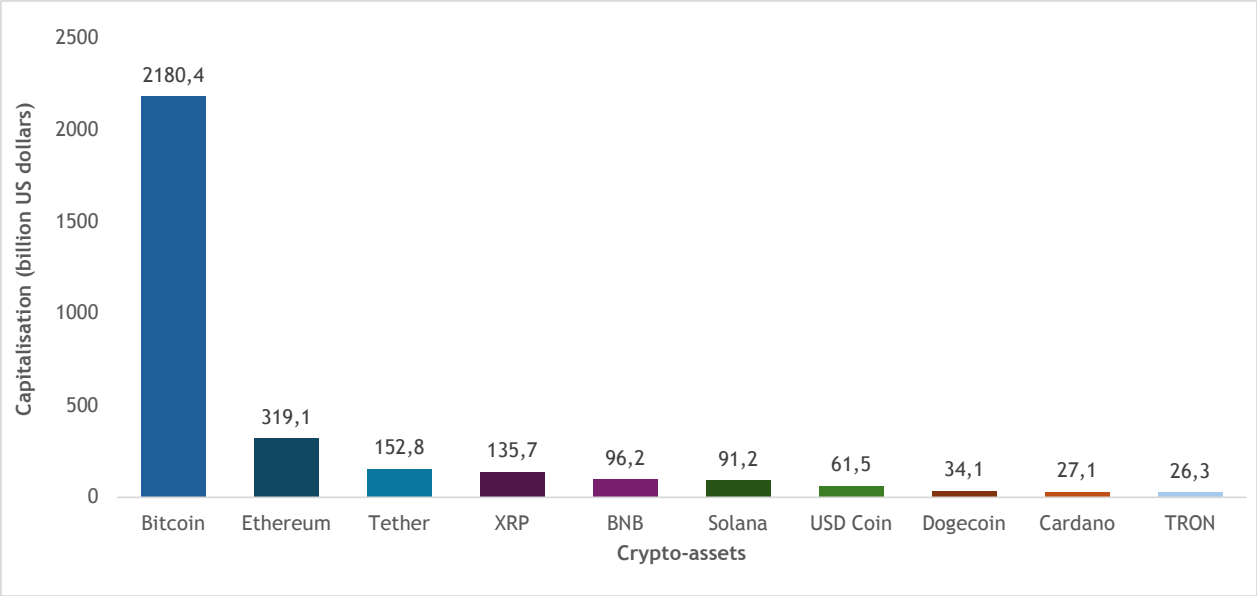
The blockchain was born just over fifteen years ago. Since then, crypto-assets have gradually and widely spread and have started to be used as means of payment. However, despite the recent introduction of regulation and supervision mechanisms, the sector — beyond the opportunities it offers — continues to pose several risks, notably in terms of money laundering and terrorist financing (ML/TF).

The persistent ML/TF risks can be explained by several factors. On one hand, they stem from a regulatory framework still in the process of being harmonised and effectively implemented (see p. 33). Key requirements such as the strengthening of user identification (Know Your Customer – KYC) and verification of the origin of funds are only just beginning to be applied consistently at the international level.

On the other hand, there are factors related to the technological features of the blockchain, which make it an immutable, uncensorable system largely outside the control of public authorities (see p. 18):

- The use of pseudonymity as a basic principle: users are identified by an address or pseudonym on the blockchain, rather than by their real identity.
- The lack of access control on most decentralised finance (DeFi) platforms, where the only requirement is connecting to a wallet. This makes traceability technically possible, but difficult and often limited in practice.
- The use of various obfuscation techniques such as bridges, mixers, chain-hopping, and other complex methods of disrupting financial flows.

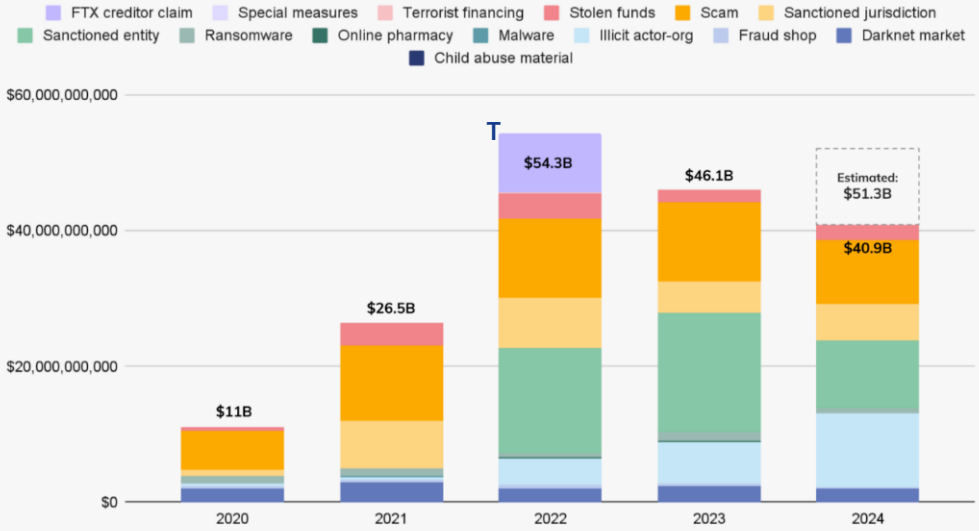
Capitalisation (number of units x observed selling price) of the main crypto assets



Source: Coinmarketcap.com, 31 May 2025

Total cryptocurrency value received by illicit addresses

2020 - 2024



Source: Blockchain.com, 31 May 2025

The use of crypto-assets for ML/TF purposes is evolving in a concerning manner, according to the most recent observations and analyses. In 2024, addresses identified as illicit received around 40.9 billion US dollars in crypto-assets, a figure that could be revised upwards to 51 billion US dollars (Chainalysis 2025 report). While this represents only 0.14% of the total volume of global crypto transactions (to be compared with the 2 to 5% of illicit transactions observed in global GDP [1]), this percentage masks the true scale of the phenomenon given how difficult it is to obtain exhaustive data in this field.

Crypto-assets have intrinsic characteristics that make them particularly attractive for money laundering, notably because of:

- No entry barriers: access to simple software and an internet connection is sufficient to carry out transactions;
- Fast, low-cost, and reliable transactions;
- Globally recognised value, facilitating cross-border use;
- A rapidly expanding international ecosystem, where many actors remain partially or non-compliant with anti-money laundering and countering financing of terrorism (AML/CFT) standards;
- A wide variety of obfuscation tools available to conceal the origin, nature, and destination of funds.

A notable trend is the increasing use of stablecoins (see p. 11), particularly in settlement mechanisms associated with money laundering stemming from drug trafficking, as illustrated by the Dark Bank case [2]. Another emerging development involves the generation of returns on illicit funds through staking protocols and other yield-generating services offered by decentralised finance platforms (see pp. 18–23).

Despite the entry into force of the Markets in Crypto-Assets Regulation (MiCA) (see p. 33), stablecoins can still easily be exchanged for privacy coins (see p. 12), either through centralised exchanges (often located outside Europe), or through decentralised finance infrastructures (see pp. 18-23), escaping any effective supervision or regulation.

In 2025, the volume of transactions carried out in stablecoins surpassed, for the first time, the volume of fiat payments processed by Visa: 27.6 trillion US dollars was settled in stablecoins, compared to 13.2 trillion US dollars via Visa in 2024 [3].

The use of bridges, which allow crypto-assets to be transferred between different blockchains, has doubled since 2022. This technique is now systematically used by the most sophisticated criminal networks to complicate the traceability of funds.

Finally, the circumvention of regulations via crypto-assets now goes beyond strictly criminal or fraudulent activities and is also part of geopolitical strategies. For instance, bitcoin transactions have reportedly been observed between Russian oil exporters and their commercial partners in Asia [4]. While the amounts remain limited for now, the strategic interest of these actors in blockchain technologies is clear.

STABLECOINS

Stablecoins are crypto-assets designed to maintain a stable value, usually pegged to a fiat currency such as the dollar or euro. While minor fluctuations — of a few percent — are common, this stability represents a notable exception in the otherwise highly volatile crypto-asset universe. For the third consecutive year, stablecoins dominate flows linked to illicit activities, accounting for 63% of criminal transactions in 2024 [5]. Their stability and ease of conversion into fiat currencies make them preferred instruments for malicious actors. They are notably used by sanctioned entities seeking to circumvent international restrictions [6].

The regulator's technical ability to control a stablecoin varies greatly depending on whether it belongs to one of the two main categories:

- **Centralised stablecoins** are issued by a regulated entity in exchange for an equivalent deposit in fiat currency or traditional assets. This entity guarantees redemption of the issued crypto-assets at a price close to their issuance cost. It also retains technical control over the assets and can freeze or seize them. The most widespread centralised stablecoins are USDT (Tether) and USDC (Circle).
- **Decentralised stablecoins**, on the other hand, are more complex. Their architecture, without a central authority, makes their control, censorship, or regulation particularly difficult (see p. 21). The most emblematic of these assets is DAI, issued via the MakerDAO protocol.

Tether (USDT)

Tether (USDT) is currently the most widely used centralised stablecoin in the world. It is issued by Tether Ltd., a company originally established in the British Virgin Islands and now domiciled in El Salvador. As of 2025, approximately 150 billion USDT have been issued.

The issuer claims to hold collateral equivalent to the total value of USDT in circulation, composed largely (around two-thirds) of U.S. Treasury bonds. However, the credibility of this claim remains controversial, particularly due to concerns over the perceived reliability of its external auditor, BDO, which may not meet the level of assurance such oversight requires (Foley, Stephen, 2024).

USDT currently operates across more than 13 different blockchains.

At this stage, European regulation — notably the MiCA Regulation — only covers centralised stablecoins, designated as "asset-reference tokens" (ARTs) or "e-money tokens" (EMTs). These stablecoins must be issued by licensed entities subject to strict requirements on transparency, reserve management, and risk management.

WALLETS AND EXCHANGES

To interact with crypto-assets, users rely on two main types of management solutions:

Non-custodial wallets

These are cryptographic software programs installed on a computer or mobile phone. These wallets offer a high degree of anonymity since they do not require formal identification. However, the user is solely responsible for the security of its funds and faces the risk of hacking of its private key stored in the wallet, which is used to sign transactions and prove ownership and authorisation to operate the wallet.

Custodial wallets via centralised platforms

In this case, users entrust the management of their assets to a third-party institution, much like a bank. These institutions offer a wide range of services: custody of funds, exchange between crypto-assets or between crypto and fiat currencies, access to financial products (futures, options, etc.), participation in decentralised protocols. The level of regulation of these institutions varies considerably, particularly based on their location.

PRIVACY COINS

It is impossible to precisely measure the use of privacy coins due to their inherently untraceable nature. These crypto-assets integrate complex and advanced cryptographic methods at all levels of their operation (see p. 18), from the dissemination of data over the peer-to-peer (P2P) network to the content of the transactions themselves, which remains encrypted and inaccessible to analysis.

Nevertheless, despite their delisting from major exchanges following the entry into force of the MiCA Regulation (see p. 33), some privacy coins — particularly Monero — continue to be significantly traded on less scrupulous platforms, such as KuCoin and HTX. As of May 2025, daily exchange volumes between Monero and USDT remain high, reaching around one hundred million euros per day.

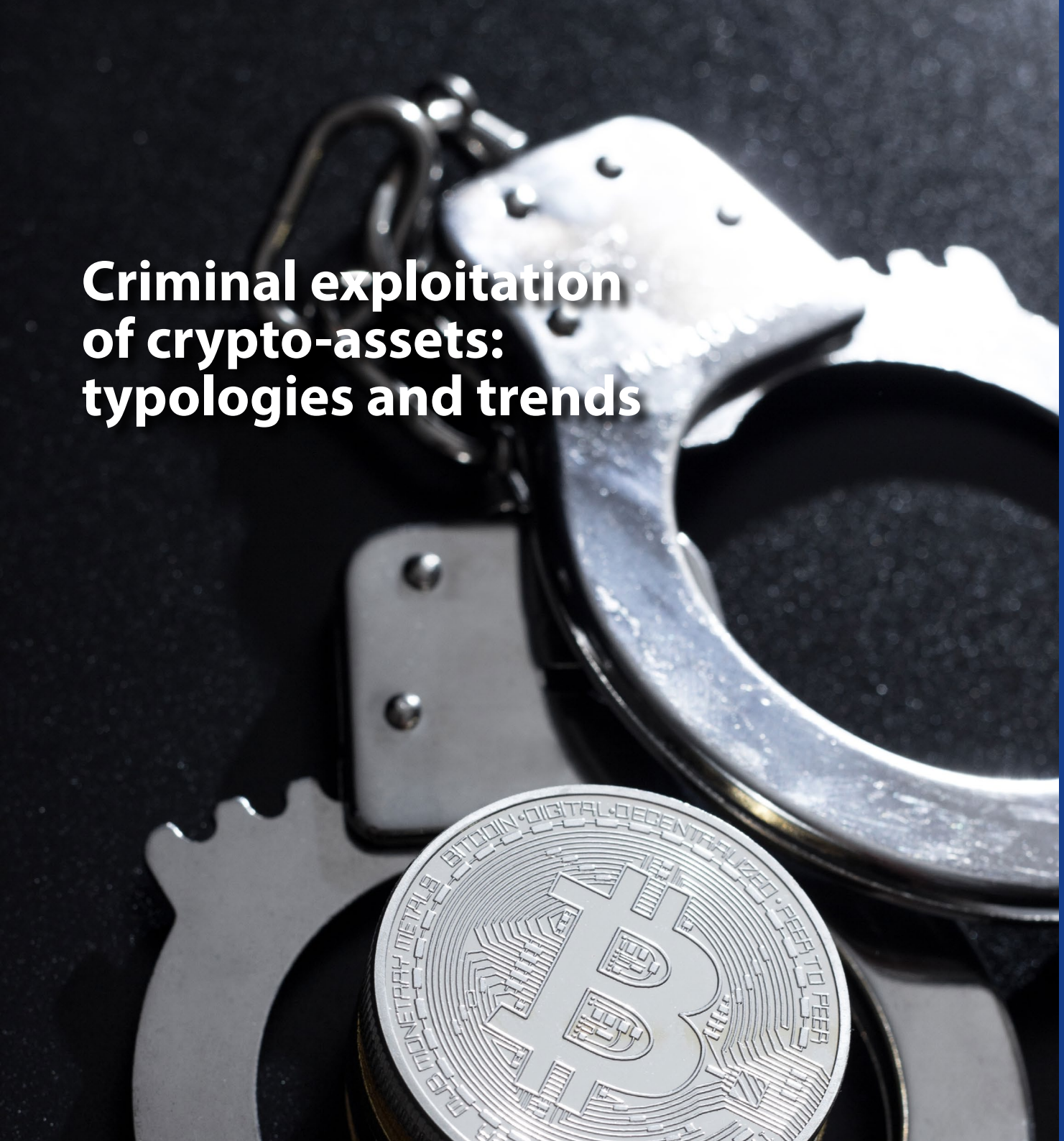
Monero

Among privacy coins, Monero stands out as the only truly significant asset in terms of adoption, technical robustness, and privacy protection. Unlike other similar assets such as Zcash, whose anonymisation features are not enabled by default, Monero's privacy features are built-in and cannot be disabled. The protocol has no known technical vulnerabilities and benefits from an active community and growing adoption.

Key characteristics of its criminal use include:

- Ransomware: The use of Monero is increasing in ransom demands (Chainalysis Team, 2022). Some criminal groups even offer discounts to victims who pay in Monero to encourage its use.
- Darknet: Monero is widely used on illicit Darknet marketplaces. Some platforms, such as White House Market, have adopted it as their sole means of payment (Chainalysis Team, 2023).
- Child sexual abuse material (CSAM): According to Chainalysis (2024), services using Monero in this domain tend to have a longer operational lifespan than those using other crypto-assets, due to the increased difficulty of tracing transactions.
- State use: There is anecdotal evidence of use by North Korea (United Nations Security Council, 2024), although its laundering methods primarily rely on stablecoins.

Criminal exploitation of crypto-assets: typologies and trends



Over the past decade, large-scale hacks targeting centralised platforms and DeFi protocols remain the most spectacular in terms of volume, with estimated losses of 2.2 billion US dollars in 2024 and 7.7 billion US dollars between 2022 and 2024 [7]. There is a growing professionalisation of operations involving transnational — sometimes state-sponsored — groups relying on dedicated infrastructures, shell companies, and encryption tools to obscure the flow of funds.

At the same time, certain criminal practices are in decline (such as the use of mixers or darknet markets), while others are gaining traction: cross-chain bridges, on-chain laundering services, and the use of artificial intelligence (AI) in targeted scams (see p. 16).

These dynamics are unfolding in a transitional regulatory context (see p. 33), where the adaptation of enforcement tools often struggles to keep pace with the speed of criminal innovation (see pp. 25–29).

THE WEIGHT OF HACKING AND CYBERCRIME

The last ten years have underscored the overwhelming importance of hacking within the criminal blockchain ecosystem, with a peak in 2022. These attacks — primarily targeting DeFi protocols, centralised exchanges (CEXs), and infrastructure — accounted for over 90% of stolen funds, totaling more than 11.6 billion US dollars (DefiLlama – Hacks, June 2025).

Among recent incidents, the February 2025 Bybit attack, with 1.46 billion US dollars stolen [8], illustrates the scale of the phenomenon.

Common techniques include the compromise of private keys or signatures, phishing, social engineering, verification bugs, and flash loan attacks (see p. 21). Rug pulls remain widespread.

Finally, the involvement of state actors in some of these attacks highlights a troubling evolution, revealing increasing geopolitical stakes around digital asset security.

DIVERSIFICATION OF CRIMES USING CRYPTO-ASSETS

While cybercrime remains dominant, the blockchain ecosystem is increasingly being used to facilitate traditional criminal activities. Transnational organised crime groups are turning to crypto-assets to commit or launder proceeds from conventional crimes such as drug trafficking, gambling, intellectual property theft, money laundering, human and wildlife trafficking, and violent crime [5].

Drug sales continue to grow, expanding beyond darknet market ecosystems into encrypted messaging apps and social media platforms like Telegram and Signal [7].

Crypto-assets are also used to circumvent international sanctions (on the rise since the tightening of sanctions), evade taxes, conduct scams, fuel underground markets, and facilitate ransomware attacks.

In 2025, several high-profile cases of kidnapping and extortion targeting internet personalities, with ransom demands in crypto-assets, drew public and governmental attention [9].

GROWING PROFESSIONALISATION AND ORGANISATION

Even with modest technical skills and limited cryptographic knowledge, criminal groups demonstrate increasing professionalism and operational sophistication.

Under mounting law enforcement pressure and evolving regulatory frameworks, criminals continuously adapt their techniques.

Decentralised finance is now fully integrated into criminal schemes (see pp. 18–23). Its characteristics

— censorship resistance, lack of a central control point, anonymity of parties — make it fertile ground for impunity.

Prosecution becomes all the more difficult as illicit flows are fragmented across multiple, often automated protocols operating outside any clear legal framework.

DECLINE OF CERTAIN PRACTICES

Some criminal trends are in decline, reflecting changing practices in the illicit crypto-asset ecosystem:

- Revenues generated by darknet markets (such as Kraken DNM, Mega, Blacksprut, OMG!OMG!, Abacus), and specialised shops (selling stolen data and personally identifiable information), have decreased over the years, despite their historical role in scams, identity theft, and ransomware campaigns.
- Use of mixers is declining in favour of cross-chain bridges.
- Scam and fraud volumes are decreasing but still represent a significant threat.

CRIMINAL ADAPTATION TO REGULATORY DEVELOPMENTS

International sanctions, the gradual compliance of major centralised exchanges (which remain highly concentrated), the emergence of strong and unified global standards, and the increasing technical proficiency of authorities are all having mixed effects on criminal behaviour.

On one hand, these dynamics push some exchanges toward weakly regulated jurisdictions, exploiting gaps or lack of adequate supervision.

On the other, they are prompting a shift in illicit activity. Criminals now rely on a wide range of hard-to-regulate tools: decentralised exchanges, cross-chain bridges, decentralised stablecoins, non-custodial wallets, etc.

These services are now routinely used — even by relatively unsophisticated criminals — and systematically chained together by more advanced groups.

In addition, the integration of off-chain practices, for instance of shell companies [10], a practice originating in traditional money laundering and terrorist financing — are now integrated with crypto-based mechanisms.

The widespread use of decentralised services by criminal groups makes analysis even more difficult due to the mixing of crypto-asset flows. This trend is reinforced by the explosion in volumes: in May 2025, crypto-to-crypto transactions via decentralised protocols represented nearly a quarter of total volume, compared to less than 10% in 2023.

This shift reflects the direct impact of regulatory pressure on centralised platforms.

USE OF ENCRYPTED MESSAGING PLATFORMS

The crypto-related crime ecosystem increasingly relies on encrypted messaging platforms, particularly Signal and Telegram. These platforms offer crypto-related services and integrate easily with non-custodial wallets.

They are used for:

- Connecting criminal service providers (Distributed Denial of service (DDoS) attacks, hacking, money laundering, etc.);
- Trading compromised databases, stolen credentials, and specialised malware;
- Technical discussions among cybercriminals;
- Illicit financing activities, including terrorism financing.

USE OF GENERATIVE ARTFICIAL INTELLIGENCE

The recent rise of generative artificial intelligence (AI) has been quickly exploited by cybercriminals to industrialise certain fraudulent practices. These tools enable:

- The creation and management of convincing fake profiles on social media;
- The execution of multiple romance scams in parallel by a single operator;
- The generation of deepfakes used in targeted sextortion campaigns;
- The automated production of spear-phishing content.

Moreover, AI also facilitates the mass generation of spam campaigns, particularly investment scams. These scams peak during bull markets in crypto-assets, amplified by media coverage and speculative hype

Pig Butchering

Romance scams, also known as "Pig Butchering", involve gaining a victim's trust over an extended period using fake profiles – often operated with generative AI tools – before convincing them to invest in fraudulent platforms, typically linked to crypto products.

This scheme is doubly exploitative, as the perpetrators communicating with the victims are often themselves held in forced labour camps in Asia.

Misuse of DeFi for money laundering/ terrorist financing purposes

THE LAYERS OF DEFI

Network Infrastructure: the communication layer

At the base, computers communicate and exchange data using the Transmission Control Protocol (TCP), regardless of their geographic or topological location.

These computers form a peer-to-peer (P2P) network. Each node is connected to several neighbors, who are themselves connected to others, forming a distributed and resilient mesh. This network enables information to be broadcast among all peers without a central coordination point.

The Blockchain: the distributed ledger technology (DLT)

On this P2P network, nodes run a cryptographic protocol that allows them to agree on the contents of a distributed (each node has a copy) and tamper-proof (no rollback possible) ledger, without a central authority or mutual trust: this is the blockchain.

The content of this ledger is constrained by the rules of the protocol. Some blockchains, like Bitcoin, only record simple financial transactions.

Others, like Ethereum, rely on autonomous programs triggered by transactions and whose execution is verified by all nodes before being recorded in the ledger. These programs are smart contracts.

Smart contracts: the logic layer

Smart contracts are software deployed on the blockchain. They define rules and actions that are executed automatically, transparently, and immutably.

The community agrees on standards for interpreting these contracts:

- A contract compliant with the ERC-20 standard is interpreted as a fungible token (e.g., a token representing a crypto-asset).
- A contract compliant with the ERC-721 standard defines a non-fungible token, a unique and individually traceable asset.

DeFi: the automation of services

Automated financial protocols are then built from these contracts:

- Uniswap is a decentralised exchange protocol simulating an order book using algorithmic functions.
- MakerDAO is a decentralised stablecoin issuance protocol.

This is the DeFi layer: an ecosystem of applications offering access to financial services (exchange, lending, borrowing, etc.) without centralised intermediaries.

User interfaces: access to services

To interact with these protocols, users rely on wallets – software that manages their cryptographic keys and allows them to sign transactions. Some are browser-integrated for easier access.

Instead of traditional identification, users are identified by a public key (a string of letters and numbers) without centralised identity management.

Websites or decentralised interfaces (dApps) use these wallets to provide intuitive interaction with DeFi protocols. They also display information stored on the blockchain, such as balances, transactions, or prices.

This visible layer represents the tip of the Web3 iceberg.

Gateways to the traditional world: centralised exchanges

Finally, centralised actors (like Binance or Coinbase) enable conversion between crypto-assets and fiat currencies. Despite the decentralised nature of crypto-assets, trading is heavily concentrated around these platforms.

They act as gateways to the traditional financial system and can be asked to provide information (KYC, history, etc.).

Decentralised finance represents a major and rapid evolution of the crypto-asset ecosystem since its emergence in the 2010s. The number of active DeFi users is constantly growing, reflecting exponential adoption and use.

However, DeFi also poses specific AML/CFT challenges. DeFi protocols offer financial services (lending, borrowing, exchanging, etc.) without centralised intermediaries, relying solely on smart contracts deployed on the blockchain.

PRAGMATISM IN THE REGULATORY APPROACH

The previous infographic highlights a subtle yet crucial point: terms like Bitcoin, stablecoins, smart contracts, exchanges, and DeFi are often used interchangeably in mainstream discourse, but in reality, they refer to fundamentally different technical constructs. The extent to which regulators can exert control over these varies significantly — from the possibility of regulating centralised exchanges under AML/CFT frameworks to the complete technical impossibility of exercising influence over decentralised swapping contracts, even though both provide similar services.

It is now widely recognised that fully automated DeFi systems operating on the blockchain fall outside the scope of current AML/CFT regulations, due to a range of structural and legal challenges.

SMART CONTRACTS

While blockchains like Bitcoin only allow asset transfers, others like Ethereum allow peers to agree on the execution of software programs.

These programs, executed globally and cryptographically verified, are uncensorable and can themselves initiate transactions.

This invulnerability makes their strength, particularly given the following characteristics:

- Transparency (from a user's perspective, not necessarily from a regulator's),
- Reliability (based on technology rather than intermediaries),
- The removal of financial intermediaries, enabling direct peer-to-peer interaction,
- Their automatic and interoperable nature with low entry barriers.

However, their use creates AML blind spots, as identity verification is not feasible. Once deployed, a smart contract is difficult — if not impossible — to regulate (see Tornado Cash, p. 23), unless the developer has embedded control mechanisms from the outset. Such mechanisms, however, are often viewed as contrary to the ethos of DeFi and may deter users. For example, centralised stablecoins such as USDT include a clause allowing the issuing entity to freeze the assets of addresses listed on sanctions lists (see p. 11). This is a clear illustration of a smart contract whose functions are tightly controlled by its developer. In such a configuration, users' trust relies more on the issuing institution than on the autonomous functioning of the smart contract itself.

By contrast, decentralised stablecoins and many DeFi protocols do not have any supervising or control authority. DeFi thus represents a form of practical deregulation of the crypto-finance sector.

Despite its technical capabilities, the complexity of DeFi often drives most users toward regulated platforms. However, for criminal groups with the necessary expertise, DeFi has become both a routine tool and a strategic asset. This was strikingly illustrated by the hacking of the Bybit platform, which revealed the operational proficiency of these actors in exploiting decentralised protocols [11].

TOKENS

Much of the DeFi ecosystem relies on tokens — crypto-assets created via smart contracts on existing blockchains.

Unlike coins (e.g., Bitcoin, Ether), which are native to a blockchain and pay transaction fees, tokens don't require a dedicated blockchain. Their issuance relies on deploying a smart contract conforming to a predefined standard — most commonly ERC-20 on Ethereum. This standard defines minimal functions for the token to be interoperable within DeFi.

Tokens are like casino chips — they only hold value attributed by their issuer or through user trust, utility, or speculation.

The USDT is technically a token. Some tokens are tied to gaming platforms, others represent scarce digital items (e.g., breeding rights for rare animals), and many have questionable "real" value.

Blockchains and crypto-assets

The first blockchain, Bitcoin, was launched in 2009. Since then, the ecosystem has grown considerably, with over 350 blockchains recorded as of early 2025. The most competitive and sustainable blockchains alongside Ethereum include Solana, BSC, Tron, Base, Arbitrum, Avalanche, Aptos, Polygon, and Cronos.

On these blockchains — which are all tamper-proof distributed ledgers — various assets are exchanged. For example, USDT, issued by the company Tether, is traded on the Ethereum, Tron, Solana, Avalanche blockchains, among others.

Each blockchain supports a native asset, which is used to pay transaction fees.

Tokens are also used in money laundering via staged transactions, profit manipulation, and flow mixing.

NON-FUNGIBLE TOKENS

Non-Fungible Tokens (NFTs) use standards like ERC-721 and ERC-1155, which differ from ERC-20 in that each token is unique and non-interchangeable. Each NFT is traceable individually from its creation through all transactions.

There are clear similarities with the luxury and art markets — such as certificates of authenticity, storing value discreetly, unique items with subjective prices, and opaque transactions. The same money laundering risks seen in those markets also apply here.

- *Overpriced purchases*: NFTs can be bought at inflated prices to justify illicit fund inflows.
- *Tax fraud*: Donating NFTs to public-interest institutions at inflated values can reduce taxable income or dodge inheritance taxes.
- *Hoarding*: Some actors mass-purchase NFTs to hold value outside the traditional banking system.

OpenSea is the leading NFT marketplace. In some collections, up to a quarter of trading volume comes from wash trading [12]. On smaller platforms (e.g., LooksRare, X2Y2 [13]), it can represent nearly all transactions. NFTs are highly suited to wash trading due to low liquidity and past speculative bubbles.

Wash trading

Wash trading involves deliberately buying and selling the same asset between accounts controlled by a single entity in order to create a false appearance of legitimate market activity. The goal is to manipulate several key market indicators: trading volume, price, and demand signals.

By falsifying these signals, the wash trader misleads other participants into believing that the asset is popular or valuable. This can prompt genuine buyers to enter the market. Once this artificial demand is created, the fraudster can sell to these real buyers at a profit, thereby completing the manipulation.

The problem is particularly widespread on low-fee blockchains like Solana.

DECENTRALISED STABLECOINS

Unlike centralised stablecoins (see p. 11), issued by companies in exchange for traditional collateral, decentralised stablecoins are issued automatically by smart contracts when users lock collateral (also in crypto-assets).

They are nearly autonomous from their creators, lack KYC, and cannot technically be censored, frozen, or seized. They face risks from crypto price volatility and potential flaws in complex smart contracts.

So far, the most significant depeg events (i.e. the decoupling of a stable crypto-asset's value from its target value) have occurred with decentralised stablecoins. However, the risks associated with centralised stablecoins should not be overlooked either. These have simply not collapsed yet, but they have occasionally experienced fluctuations of up to 20% over the course of several days.

UST and LUNA

UST was a decentralised stablecoin that collapsed, wiping out 45 billion US dollars in crypto market capitalisation. When UST fell below 1 dollar, users could buy it cheaply, exchange it via a smart contract for 1 dollar worth of LUNA, and then sell that LUNA to make a profit.

However, the sharp drop in UST triggered massive arbitrage, leading the contract to generate a large amount of LUNA. This sudden supply increase drove down LUNA's price, which in turn caused the contract to issue even more LUNA for every new UST input by arbiters. This cycle continued until LUNA's supply exploded and its price collapsed—making it impossible for UST to regain its target price of 1 dollar.

FLASH LOANS

Flash loans are a unique feature of DeFi that allow users to borrow large amounts of crypto-assets without providing any collateral, via a smart contract. The only condition is that both the loan and its repayment — including fees —must be fully executed within a single transaction. This transaction may include multiple sub-transactions, but the process is atomic: either all steps succeed, or the entire transaction is reverted.

Originally designed to enable arbitrage opportunities, flash loans have also been misused for malicious purposes, particularly in attacks exploiting smart contract vulnerabilities.

For example, in the Platypus case, an attacker exploited a flaw in a decentralised stablecoin protocol (USP), combining flash loans, collateral manipulation, and a bug in the contract to siphon off funds — leading to a partial loss of value for the asset.

DECENTRALISED EXCHANGES

The most well-known DeFi applications are decentralised exchanges (DEXs) and liquidity protocols. EtherDelta was the first DEX (2017), later surpassed by Uniswap, and more recently (May 2025) by PancakeSwap.

These contracts allow anyone to exchange tokens. Creators can only marginally alter their behavior (e.g., by handling fees), making seizure, blocking, or sanctions technically impossible.

UNISWAP

A decentralised exchange protocol that algorithmically simulates an order book; users influence the exchange rate based on the tokens they trade, and investors participating in governance make decisions — for example, regarding fees.

MakerDAO

The first decentralised stablecoin issuance protocol. Investors can decide on the parameters of the collateral algorithm that backs the stablecoins with fiat-equivalent value.

BRIDGES

Another functionality offered by crypto-asset service providers (CASPs) and replicated by DeFi is the ability to exchange two crypto-assets not within the same blockchain, as is the case with DEXs, but between two different blockchains (for example, Bitcoin for Ether).

Bridges are autonomous systems that operate securely and without any KYC requirements.

They have legitimate uses, notably allowing users to carry out exchanges or manage complex products on faster blockchains where fees are lower. However, they are also used by skilled criminal groups to delay the analysis of flows. North Korea (the «Lazarus» group) now uses this technique [14].

MIXERS

Criminals also exploit crypto-asset mixers. These are services that mix the funds of many users before redistributing them, making traceability very difficult.

These services have no equivalent in the traditional financial system. The French authorities have become aware of these risks. Thus, in France, their use explicitly falls under Article 324-1-1 of the Penal Code on the presumption of money laundering, which reverses the burden of proof and presumes that funds passing through a mixer come from a crime or offence.

These tools, although having a legitimate use linked to financial privacy, are misused to conceal the connection between wallets collecting illicit funds and those used to transfer funds to exchange platforms.

Tornado Cash

Tornado Cash is a decentralised mixer that has allowed, since 2019, the anonymisation of transactions on the Ethereum blockchain by automatically obscuring the links between sending and receiving addresses through advanced cryptography (Zero-Knowledge Proof).

An international judicial response in 2022–2023 led to the arrest of individuals involved in the project and the shutdown of associated accounts on technical platforms.

However, on the one hand, the Tornado Cash smart contract (see p. 19) continued — and still continues — to function, as it is impossible even for States to censor it. On the other hand, the U.S. sanctions against Tornado Cash were lifted by the American administration.

This example clearly illustrates the challenges posed by decentralised finance: despite a successful law enforcement action, including multiple arrests, seizures, and shutdowns, the money laundering system remains operational.

THE DEFI

Systemic, technological, money laundering and terrorist financing risks are evident on DeFi platforms. In terms of AML/CFT requirements, the absence of identity verification procedures (KYC) in decentralised exchanges represents a major vulnerability, allowing for relatively confidential and hard-to-trace transactions. In this context, it is important to highlight that there is not always a correlation between the level of crypto-asset adoption in a given country and the maturity of its regulatory framework. For example, several jurisdictions positioned as crypto-industry hubs — such as Singapore, Hong Kong, the United Arab Emirates, or Switzerland — actually have a relatively low national adoption rate.

Recently, a ruling was issued in the United States regarding the exploitation of a vulnerability on a DeFi platform (Mango Markets), which allowed a malicious actor to manipulate the price of the token used by the platform — Mango (MNGO) — in order to borrow the equivalent of 110 million US dollars in crypto-assets without ever repaying them. The landmark ruling sided with the actor, with the judge stating that he had merely exploited the computer code and was not responsible if it was poorly written.

In other words, to quote a popular saying in the crypto-asset world: *"Code is Law."*

Development of investigative tools and techniques to deal with crypto-crime

The success of investigations relies on a close combination of advanced technical expertise and an appropriate legal framework. This synergy enables the tracing of financial flows, the partial lifting of the anonymity of certain wallets, and, when necessary, the seizure of crypto-assets.

Among the tools specific to blockchain analysis, there are mainly two categories. On the one hand, block explorers, which offer a graphical interface — more or less sophisticated — allowing users to explore the contents of the transaction ledger. On the other hand, blockchain analysis tools (see p. 26), which go further by capturing additional information, grouping and de-anonymising certain transactions, among other capabilities.

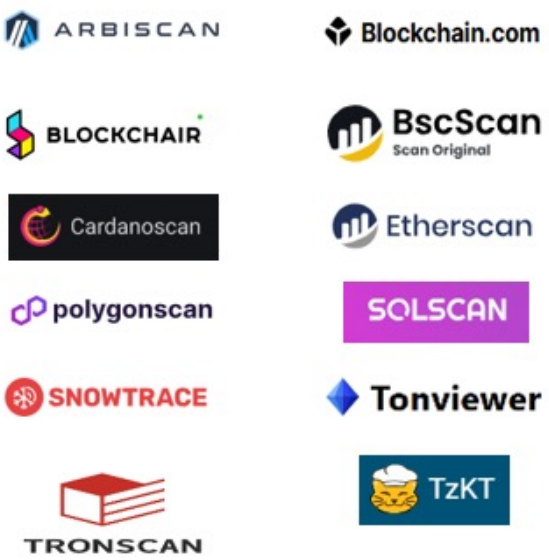
However, these tools alone are not sufficient to equip a Financial Intelligence Unit (FIU) with the investigative capacity it needs. They must be combined with other sources of information, such as data provided by obliged entities (e.g. suspicious transaction reports or disclosures obtained through the right to communication), intelligence gathered from social networks, and open-source information (see p. 27).

BLOCK EXPLORERS

A block explorer is a web interface that allows real-time or retrospective consultation of the data recorded on a blockchain: transactions, addresses, blocks, smart contracts, or other elements.

For investigators, these tools are a valuable entry point. They allow for quick tracing of simple flows between addresses, checking transaction details (amount, timestamp, sender and recipient), tracking basic interactions with a smart contract — even viewing its source code — and identifying movement patterns or interactions with known entities. These observations can then be cross-checked with other intelligence sources or analysis tools to refine the investigation.

Free explorers should therefore not be overlooked. Some, such as Etherscan, provide access to much more detailed information than commercial explorers (for example, concerning smart contract data and their code). As such, they offer both educational value and forensic capabilities useful to FIUs and other competent authorities.



BLOCKCHAIN ANALYSIS TOOLS

Investigations into crypto-asset transactions now rely on blockchain analysis tools, which are the main technological innovation in this field. These tools exploit a node of one or several blockchains to access data and track transactions in real time.

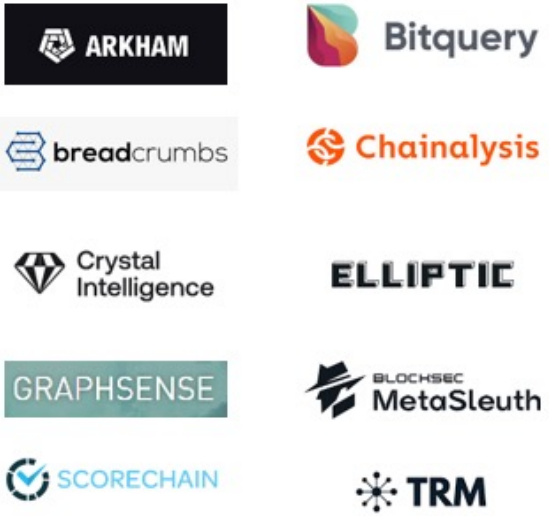
Beyond the functionalities offered by block explorers, blockchain analysis tools enable exploitation of blockchain data over long periods and on a large scale. By combining advanced cross-referencing techniques, they perform behavioural analysis of an address linked to a crypto-asset wallet. They allow the clustering of addresses (see p. 28), identification of high-risk wallets, generation of alerts, and assistance in retracing the path of suspicious funds.

The use of these tools is therefore indispensable today for crypto-asset investigations. They represent a critical link in the intelligence chain, allowing analysts to move from pseudonymous transaction flows to concrete, actionable leads.

A few examples of available market solutions are presented on p. 27. Among them, GraphSense is the only open-source tool.

Commercial tools
Open source tools

Category	+	Benefits	-	Disadvantages
Use	✓	Free access and immediate use	☒	Approval for use
Clustering	✓	Clustering, use of group or batch processing algorithms	☒	No clustering, weak identification according to block explorers
Identification of services	✓	Identification of services	☒	Non-exhaustive identification/clustering (unpublished methods)
			☒	Limited analytical and identification capabilities
Additional information	✓	Adding data (OSINT, IP addresses...)	☒	Does not support all existing blockchains
			☒	Additional information missing
Update	✓	Regular updates	☒	Random updates
Interface	✓	Graphical interface	☒	No graphical tracking on most free tools
Customer support	✓	Customer support	☒	No customer support
Help service	✓	Support services (survey, technical.)	☒	Rather absence of such services
Cost	✓	Rather free by nature	☒	High and expensive cost in implementation (including subscription, customisation, integration and additional customer support)
Reliability of data	✓	High reliability and precision		
	✓	Progressive reliability of block explorer data		
Sovereignty of data	✓	Open source data that can be verified by everyone	☒	Non-sovereign tool (data collected by the operator and abroad, often in the United States)



OPEN-SOURCE INTELLIGENCE

The investigation cannot be limited to on-chain data alone. A large amount of complementary information, called metadata, is essential to enrich the analysis. Some of it is collected by blockchain analysis tools, which make it usable via their interfaces. Others can be obtained by operating one or more nodes of the P2P network underlying the blockchain (see p. 18).

This data can be cross-referenced with attacks on anonymisation networks (such as the Onion Routing project or TOR) or via information requests sent to virtual private network (VPN) providers, which are almost systematically used by criminals.

In addition, cybercrime units also use techniques such as open-source intelligence (OSINT) and clustering (a data analysis technique that involves grouping sets of objects that share similar characteristics) to identify users behind pseudonymous wallets.

These methods are especially useful when attempting to reconstruct deliberately obscured ownership chains — e.g., via mixers or by passing through exchange platforms.

A concrete example of OSINT/on-chain cross-analysis consists of leveraging the presence of Ethereum Name Service (ENS) names on social networks. Many Twitter accounts mention their ENS address, making it possible — by correlating Twitter data with the blockchain transactions linked to those addresses — to surface attribution leads or even identify the beneficial owners of certain transactions.

ENS: Ethereum Name Service

Domain names are managed by centralised organisations, often state-affiliated (e.g., AFNIC in France for managing .fr domains).

In contrast, ENS is a DeFi system on the Ethereum blockchain, which allows the assignment of domain names (ending with .eth) independently of any central authority.

Similarly, some criminals try to transfer their reputation from one platform to another by reusing the same pseudonym or a recognisable variation. This practice is particularly common on darknet marketplaces. Cross-analysis of these aliases can help establish links between several digital identities, map criminal networks, or even attribute activities to a single individual or group.

CLUSTERING

One of the most important added values of blockchain analysis tools — beyond their intuitive graphical interface — is their ability to automatically group addresses controlled by the same entity.

On blockchains based on the UTXO model (like Bitcoin and its derivatives — see text box), each transaction includes one or more outputs destined for the recipient, but often also includes a "change address", to which the sender redirects the remaining balance. This change address, also controlled by the sender, allows for recovery of the excess from the transaction.

The ability to correctly identify the change address is a crucial step to group, with a high degree of probability, the addresses belonging to the same user. This process is based on heuristic techniques, i.e., analysis rules based on typical behavioural patterns.

Some of these heuristic techniques, well established and considered reliable, are integrated into commercial solutions. Others, more uncertain, may nonetheless prove relevant when cross-referenced with other sources or indicators, thus enabling the tracking of flows with a high level of confidence, even in complex situations.

This approach forms the basis of clustering, a fundamental analysis technique that significantly reduces the complexity of transaction graphs. It facilitates the reconstruction of fund trajectories and the identification of involved actors.

However, it should be noted that commercial solution providers do not publish the heuristics they use for clustering, both to preserve their competitive advantage and to avoid the development of countermeasures.

This lack of transparency may pose problems in the context of digital evidence, especially in criminal proceedings, if the validity of the analysis is contested.

This type of analysis therefore requires advanced technical expertise. It is essential that specialised investigators be trained to apply these heuristics and be able, when necessary, to go beyond the capabilities of standard commercial tools.

UTXO: the Bitcoin Transaction Model

Unlike Ethereum, Bitcoin does not use an account-based system with a single balance, like a bank account. Instead, it relies on a model called UTXO (*Unspent Transaction Output*).

In this system, each transaction is composed of:

- inputs: the funds received from one or more previous transactions,
- outputs: the funds sent to one or more addresses.

Inputs must be fully spent in a new transaction; it is not possible to spend only part of an input. When the amount received is greater than the amount to be transferred, the transaction must include:

- one output to the recipient,
- another output to an address controlled by the sender (often called a change address).

The difference between the total amount of the inputs and the total amount of the outputs corresponds to the transaction fee paid to miners.

IDENTIFICATION OF EXCHANGE PLATFORMS

Another major advantage of blockchain analysis tools lies in their extensive databases of addresses associated with exchange platforms.

A key investigative technique is to identify, as early as possible, financial flows entering or leaving a regulated exchange. When such a link is established, the concerned platform can — depending on the applicable legal framework — freeze the funds or transmit identifying information about the wallet holder to competent authorities (KYC data, transaction history, IP addresses, etc.).

However, from the sole perspective of on-chain data, there is no inherent way to distinguish an address created by an average user from that of a centralised exchange (even though the usage patterns may differ greatly). It is therefore crucial to be able to identify the addresses of exchanges.

Public block explorers list some of these addresses, but the most advanced blockchain analysis tools go further: regulated platforms themselves now directly communicate their address ranges to blockchain analysis tool providers.

Impact, outlook and future directions for Financial Intelligence Units

The emergence of crypto-assets has profoundly transformed the operational environment of Financial Intelligence Units, introducing new regulatory, technological, and human challenges. These issues require the continuous revision of FIU practices, tools, and partnerships to enable them to respond effectively to constantly evolving financial threats.

A first major challenge was to bring exchange platforms under AML/CFT legislation. In France, this materialised in 2019 with the introduction of the regime for CASPs, followed at the European level by the entry into force of the MiCA Regulation and the creation of the CASP status. This harmonised framework constitutes significant progress toward better supervision of the sector.

A second, more structural issue has been encouraging these actors to obtain registration, comply with regulatory obligations, and submit high-quality suspicious transaction reports. This objective has faced two main obstacles:

- on one hand, the absence of a compliance culture in a sector that is technically accessible without prior authorisation;
- On the other hand, a founding ideology — the cypherpunk movement — has historically been hostile to any form of institutional supervision.

While this has been partially overcome within the European Union, some platforms have long applied minimalist KYC procedures or even concealed their location to escape regulators. In many jurisdictions still lacking a specific framework, these difficulties persist, hindering FIUs' ability to collect and effectively exploit financial data.

Despite regulatory advances, FIUs must still overcome major operational challenges. They largely depend on commercial blockchain analytics tools, which are often expensive and developed by foreign companies — raising concerns about sovereignty and security. Furthermore, the expertise required for analysing crypto flows involves rare and highly sought-after skills, complicating efforts in recruitment, training, and retention.

CHALLENGES POSED BY THE DEVELOPMENT OF THE CRYPTO ECOSYSTEM

Evolution of the FIUs' operational environment

The proportion of illicit transactions among crypto-asset transactions tends to decrease, but the absolute value continues to rise. The harmonisation of European regulation requires providers to collect identifying data from their clients, and the strong market concentration naturally drives the vast majority of them to comply. Moreover, the immutable and permanent nature of the transaction ledger allows for an exploitable public trace of all flows, and the commercial offer of tools to leverage it is growing rapidly.

The Westphalian vision of state sovereignty over its territory [15] finds a definitive counter-example in the blockchain — and particularly in DeFi — where users pushed out of regulated platforms by KYC requirements seek refuge (see Tornado Cash text box for a concrete example, p. 23). Tax havens and non-compliant jurisdictions also host numerous operators, thereby evading regulatory obligations.

Technical projects based on blockchain are multiplying and becoming increasingly complex, while reliable technical information about them remains difficult to identify and interpret. This difficulty is exacerbated by the inherently ephemeral nature of the information, due to the rapid pace of technological evolution.

Challenges in data collection and exploitation

FIUs can hardly avoid equipping themselves with blockchain analysis tools. Unfortunately, these tools are costly and, above all, not sovereign — leading to strong and troubling dependence on a small number of commercial actors, whose affiliations are sometimes suspected of being linked

to the intelligence services of the countries where they are based. It seems urgent for European states to develop sovereign tools. However, this ambition faces many obstacles, including at times a lack of political will, largely due to a persistent misunderstanding of the nature of blockchains at the highest levels of government.

Additionally, it is complex for FIUs to benefit from data seizures carried out by law enforcement. These seizures — such as that of the BTC-E exchanger in the late 2010s — often make it possible to unravel mixer transactions, leading to cascading case resolutions and severe blows to the criminal ecosystem. More cooperation in this area should be encouraged. Crypto-related investigative data shared by law enforcement across Europe via Europol's SIENA platform could be highly valuable to FIUs.

Public-private partnerships

DeFi in its purest form will remain, by nature, beyond the reach of state jurisdictions. The progressive migration of laundering flows toward DeFi operators demonstrates the effectiveness of emerging European regulatory harmonisation. Nonetheless, further efforts can and should be made to increase pressure on still-accessible centralised vectors.

It is particularly crucial to streamline and accelerate asset-freezing procedures, by identifying the appropriate technical counterparts at obliged exchange platforms or stablecoins operators. To ensure real effectiveness, the time between detection of a criminal flow and the execution of a freeze should ideally be reduced to a few hours — or even minutes — versus the current delay of several days or even weeks.

FIUs could also benefit from an integrated intelligence network that includes contributions from the private sector, following a logic of co-construction and sharing of financial intelligence.

Evolution of reporting and information sharing

The volume of suspicious transaction reports related to crypto-assets in Europe is steadily increasing. However, their quality remains inconsistent: the information is often poorly standardised, sometimes incomplete or inaccurately filled out, which significantly limits its usability. The relevance of the reports also varies depending on the reporting entity.

Data submitted by CASPs is frequently poorly calibrated, fluctuating between excessive granularity and overly vague reports. Better training of obliged entities is therefore essential to enhance their ability to detect and report suspicious behaviour effectively.

Standardising these reports at the European level and using a common format for querying and sharing between FIUs, are essential steps toward effective cooperation. However, this standardisation must not come at the expense of experience-based practices developed by the most advanced FIUs in the field of crypto-assets.

Automatic detection and AI-based detection

Machine learning tools can be usefully deployed based on raw blockchain data, suspicious transaction reports, or directly at the operator level. The latter case mostly requires the establishment of public-private partnerships, as well as a clear definition of target behaviours to detect. These tools enable the automatic generation of alerts based on known money laundering typologies.

Additionally, obliged entities must acquire tools capable of identifying AI-generated fake identity documents — which are becoming increasingly convincing — and triggering corresponding automated alerts.

Training, triage and prioritisation

Even if FIUs had comprehensive, clean, and usable data and high-performance tools, the scale of the

phenomenon requires rigorous management of human constraints.

It is essential to continue and intensify training efforts for investigators and their support teams, while encouraging recruitment or internal specialisation of staff on crypto-asset-related matters. At the same time, mechanisms for triaging and prioritising cases should be put in place, based on clear and measurable objectives, to maximise the operational impact of available resources.

STRENGTHENING THE EUROPEAN AML/CFT FRAMEWORK

The adoption of the MiCA Regulation marks a key step in structuring the crypto-asset market within the European Union. This harmonised framework now governs crypto-asset issuers, CASPs, and markets, setting requirements in terms of transparency, governance, and consumer protection.

In parallel, the extension of the Travel Rule (requiring the transmission of information on originators and beneficiaries) to crypto-asset transfers enhances transaction traceability and the ability of competent authorities to detect suspicious flows. These instruments are complementary and aim to adapt the AML/CFT arsenal to the specifics of Web3 (the decentralised version of the Internet based on blockchain).

However, decentralised applications remain, for now, outside the scope of MiCA. In the coming years, the European Commission will need to assess whether to develop a regulatory framework adapted to these new models. Unlike the European approach, which leans toward a general regulatory framework for DeFi (to be defined: tailored, modular, *ad hoc*, or sectoral), U.S. authorities tend to favour case-by-case regulation, often through litigation.

Traditional compliance methods — based on the identification of a responsible legal person responsible, centralised monitoring, and *ex ante* obligations — are poorly suited to decentralised architectures. Effective regulation of DeFi will therefore need to take into account several parameters:

- the need for legislative flexibility to anticipate technological evolution;
- a focus on user interfaces and economic operations, rather than on the code itself or the underlying technologies;
- risk management mechanisms covering governance, cybersecurity, infrastructure, services and oracle issues;
- the possible implementation of a certification or voluntary registration system for financial-purpose protocols.

Additionally, the creation of the EU Anti-Money Laundering Authority (AMLA) represents another decisive advancement. With a supranational mandate, this independent authority will be responsible for ensuring consistent application of AML/CFT rules across the Union and will play a central role in coordinating FIUs and national supervisors. It will also help facilitate cross-border cooperation and directly supervise certain high-risk actors, including those operating in the crypto-asset sector.

STRENGTHENING COOPERATION WITH CRYPTO-ASSET SERVICE PROVIDERS

Beyond legal and institutional tools, strengthening cooperation with crypto-asset service providers is a fundamental pillar of effective AML/CFT. Raising awareness among these actors of money laundering typologies, tax fraud methods, and FIU expectations aims to improve the quality and relevance of suspicious transaction reports while facilitating constructive dialogue with the private sector.

This cooperation is especially essential given that many obliged professions still have significant room for improvement in their understanding of crypto-asset-related risks. Some financial

institutions struggle to identify operations involving these assets within their own systems, particularly in cases where:

- a customer feeds an account opened with a CASP via a bank card;
- a wire transfer is made to a CASP, sometimes via an intermediary payment provider between the bank and the platform.

This lack of visibility hampers the detection of crypto-asset-related flows and undermines the quality of monitoring mechanisms.

However, specialised payment service providers for the crypto industry are emerging, such as those offering virtual IBANs to CASPs. Identifying these actors and establishing dedicated cooperation channels with them could serve as a valuable operational lever to strengthen the detection and reporting chain.

INTERNATIONAL COOPERATION: AN IMPERATIVE TO ADDRESS CRYPTO-RELATED AML/CFT CHALLENGES

In the realm of international cooperation, one of the main challenges is the difficulty of linking crypto-asset flows to a specific jurisdiction.

Unlike a bank account, which is inherently linked to the jurisdiction that licensed the account-holding institution, a crypto-asset address visible on a blockchain can be associated with any country. This issue arises even in the case of addresses linked to exchange platforms or, more broadly, regulated entities. For instance, if investigators establish a link between an offense and a CASP that holds licenses in multiple jurisdictions, it won't be easy to determine which partner FIU should be contacted first.

This complexity is compounded by the fact that the headquarters or operational base of some platforms is sometimes unclear or intentionally obscured.

In this context, international cooperation plays a key role in enabling a coordinated response to these issues. It could notably facilitate systematic information-sharing about the jurisdictions of establishment of major sector players and their regulatory scopes.

The cross-border nature of crypto-assets indeed requires enhanced cooperation between FIUs. At the European level, such cooperation is now taking a more structured form thanks to the new regulatory framework on AML/CFT, which aims to strengthen collaboration among member states while integrating the specificities of crypto-assets. This coordination is all the more crucial given that the financial flows associated with these assets far exceed national borders.

Technical bottlenecks

The exchange of intelligence, access to specialised technical expertise, and sharing of experience among FIUs are essential to keep pace with the rapid evolution of AML/CFT typologies involving crypto-assets. However, several technical obstacles still hinder this cooperation.

One major issue lies in the heterogeneity of formats in which crypto-asset-related information is received. To date, only a minority of reporting entities use the digital reporting systems implemented by FIUs. In many cases, reports are still submitted via email or even on paper, complicating processing, reducing data usability, and slowing automated analysis capabilities.

This lack of standardisation also hinders interoperability between FIUs, limits cross-border information sharing, and negatively affects responsiveness in handling suspicious financial flows. Greater efforts are needed in standardising formats, improving technical tooling, and investing in advanced analytics solutions to overcome these bottlenecks.

State-sponsored attacks

The threat does not only stem from criminal groups or private actors. Some states or state-backed entities are actively hostile toward the international financial order.

The hacking of the Bybit platform attributed to actors affiliated with North Korea [16], as well as the use of certain Russian platforms as actual laundering hubs for digital assets [17], illustrate this worrying trend. These activities are not merely cases of non-cooperation but rather deliberate strategies aimed at financing illicit activities — such as weapons programs — or evading international sanctions.

Faced with this reality, FIUs and competent authorities must adapt their posture by recognising that certain risks stem from state-level threats. This implies strengthening international coordination, supporting financial cyber-defence mechanisms, and increasing vigilance in identifying crypto flows associated with hostile state actors.

CONCLUSION

The decentralised finance ecosystem is evolving rapidly and presents a technical complexity that makes its regulation particularly difficult. While certain centralised actors can be subject to regulatory controls and constraints, smart contracts — autonomous and censorship-resistant — largely escape any form of traditional oversight. Mastery of these systems requires highly specialised skills, which gives an advantage to sophisticated criminal groups, while authorities struggle to impose effective compliance measures, thereby exacerbating the challenges related to monitoring and controlling this constantly evolving financial universe.

In this shifting context, FIUs are confronted with a multitude of technological, organisational, and human challenges. Access to relevant data, its interpretation, the training of personnel, the development of sovereign tools, and cooperation with crypto-asset service providers have all become unavoidable requirements. The quality of suspicious transaction reports, the capacity to exploit weak signals from blockchains, and the ability to act swiftly to freeze assets are all critical factors for ensuring the effectiveness of efforts to combat illicit financial flows. These requirements demand a profound transformation of FIU working methods, a strengthening of their partnerships — both public and private — and a clear recognition of their strategic role in the financial security ecosystem.

Given the scale and transnational nature of the threats, the future of the fight against money laundering and terrorist financing linked to crypto-assets depends on intensified cooperation between FIUs, both at the European and international levels. The standardisation of exchange formats, the sharing of technical expertise, coordinated responses to state-sponsored threats, and mutual access to powerful tools are all essential levers for collectively confronting financial flows that transcend borders. Although significant progress has been made, notably through the MiCA framework and the growing role of AMLA, the consolidation of this architecture still depends on strong political will and sustained investment. For only lasting mobilisation will make it possible to preserve the integrity of the financial system in the face of the profound changes introduced by blockchain technologies.

Annexes

GLOSSARY

Blockchain: A blockchain is a decentralised, distributed ledger that records data in sequential, append-only blocks. Each new block, linked to the previous one via a cryptographic hash, is added through consensus among network nodes. Invented by Haber and Stornetta in 1991, it underpins crypto-assets. The ledger's history is immutable, transparent, and typically open source.

Bridge: A protocol enabling the transfer of assets and data across different blockchain networks, either unidirectionally or bidirectionally, without relying on centralised intermediaries.

Chain-hopping: The technique of rapidly converting and moving crypto-assets across different blockchains to obfuscate their origin, often using bridges, decentralised exchanges, or swap protocols.

Clustering: A data analysis technique used to group similar objects. In crypto analysis, clustering links multiple addresses or wallets to a single entity based on transactional patterns.

Custodial / Non-custodial: A custodial service manages and stores users' private keys, typically accessible via a username and password, providing security and asset recovery. Centralised exchanges are common custodial services. Non-custodial use refers to users managing their own private keys independently of third parties.

Cross-chain bridge: A mechanism connecting distinct blockchains, allowing the exchange of data and assets between them. Use cases include cross-chain oracles, asset transfers, and inter-chain smart contract interactions.

Crypto-asset: A crypto-asset is a digital asset secured by cryptography and recorded on a blockchain, where transactions are validated by decentralised participants. It includes cryptocurrencies, non-fungible tokens (NFTs), stablecoins, and security tokens.

Darknet: A part of the internet not indexed by standard search engines and accessible only through anonymising tools like Tor. Darknet marketplaces commonly use crypto-assets for illicit transactions.

Deepfake: AI-generated synthetic media that convincingly impersonates individuals' voices or appearances. Deepfakes can be weaponised for fraud, identity theft, misinformation, or privacy violations.

Depeg: Occurs when a stablecoin deviates from its pegged value (e.g., 1 US dollar), either by falling below or exceeding the reference asset, often indicating instability in the mechanism maintaining the peg.

Distributed Ledger Technologies (DLT): A distributed ledger technology is simply a decentralised database managed by multiple participants. It records the history of transactions across nodes in a decentralised manner. Each node validates and records transactions simultaneously. Records are time-stamped and must include a cryptographic signature, which ensures the security and integrity of the network. A blockchain is a specific type of DLT.

Ethereum Name Service (ENS): A decentralised naming protocol replacing complex Ethereum wallet addresses with human-readable domain names (e.g., "kathe.eth"), improving usability and reducing errors.

Flash loan: A loan taken from a smart contract liquidity pool without collateral, provided it is borrowed and repaid within a single blockchain transaction. Commonly used for arbitrage, but also prone to exploit.

Hacking: The unauthorised access to crypto wallets or exchanges, often with the intent to steal funds or exploit system vulnerabilities.

Mixer: A service that blends crypto-assets from various users to obscure the source and ownership

of funds, often used to enhance anonymity or launder illicit assets.

Non-Fungible Token (NFT): A unique crypto-asset that is not interchangeable with another due to its distinct characteristics (e.g., digital art, collectibles). Unlike fungible assets, each NFT has individual value and properties.

On-chain: Refers to transactions recorded directly on a blockchain, verifiable and immutable. In contrast, "off-chain" transactions occur outside the main blockchain and may lack the same security guarantees.

Open-source intelligence (OSINT): In the crypto-asset context, OSINT refers to the use of publicly available tools and techniques to investigate blockchain activity, trace suspicious behaviour, and attribute addresses.

Oracle: In the crypto-asset and blockchain ecosystem, an oracle is a third-party agent or service that delivers external data to a blockchain or smart contracts. These intermediaries are necessary because blockchains cannot natively access external data due to their secure and decentralised design.

Pig butchering: A type of investment scam in which fraudsters assume false identities to deceive and lure victims online. Using social engineering techniques, artificial intelligence, and other technologies, they build trust, emotionally manipulate targets, and exploit financial vulnerabilities to steal money.

Privacy coins: A type of crypto-asset designed to conceal transaction details such as sender, recipient, amount, and account balances, thereby offering enhanced anonymity.

Rug pull: A scam where project developers abruptly withdraw investor funds and abandon a project, typically after generating hype and inflating token value — similar to a Ponzi scheme.

Smart contract: A smart contract is a self-executing code or agreement stored on a blockchain, which automatically enforces predefined conditions without third-party intervention when the agreed criteria are met.

Spear Phishing: A targeted phishing attack that tricks individuals into clicking on malicious links, often via personalised emails designed to steal credentials or deploy malware.

Stablecoin: A crypto-asset designed to maintain a fixed value relative to a reference asset (e.g., fiat currencies like the US dollar in USDC, or other crypto-assets like DAI). Stability may be achieved through collateralisation or algorithmic mechanisms.

Staking: The act of locking a quantity of crypto-assets to participate in transaction validation on a proof-of-stake blockchain network. Validators earn rewards but may lose staked assets for misconduct or underperformance.

Swapping: The process of converting one token into another, typically via a decentralised exchange or swap platform.

Token: A blockchain-based digital unit representing value, utility, or ownership, built on an existing blockchain (e.g., Ethereum). Tokens differ from native assets (like ETH or BTC), which are intrinsic to their respective blockchains.

Travel Rule: A FATF requirement mandating Virtual Asset Service Providers (VASPs) to collect, store, and transmit originator and beneficiary information for transactions above a certain threshold. This rule applies only to regulated entities, not to peer-to-peer or unhosted wallet transactions.

Unspent Transaction Output (UTXO): A term used to describe a transaction output that has not yet been spent. Not all blockchains use the UTXO model, but Bitcoin does. In Bitcoin, each transaction consists of one or more inputs and outputs, with each input being the output of a previous transaction — except in the specific case of new bitcoins being created with each block.

Virtual Private Network (VPN): A technology that encrypts internet traffic and masks user identity and location, enhancing online privacy and circumventing censorship or surveillance.

Wallet: A digital tool for generating, storing, and using cryptographic key pairs. Wallets can be hot (connected to the internet) or cold (offline), and custodial (managed by a third party) or non-custodial (user-controlled).

Wash Trading: A market manipulation practice in which the same entity buys and sells the same asset to create artificial trading volume or influence prices.

Zero-Knowledge Proof (ZKP): A cryptographic protocol enabling one party to prove the truth of a statement without revealing any underlying data. For example, it can verify someone's identity without disclosing personal details.

BIBLIOGRAPHY

1. United Nations Office on Drugs and Crime (2011), "Estimating illicit financial flows resulting from drug trafficking and other transnational organised crimes", UNODC, Vienna, [accessed 11 June 2025]. Format PDF. Available at: www.health.qld.gov.au/phs/cphun/8887_doc.pdf. www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.
2. Abdelhak El Idrissi (2025), "The fall of Dark Bank, the organised crime 'banker' who allegedly helped launder more than EUR 1 billion", *Le Monde,* January 2025, [accessed 11 June 2025], available at: www.lemonde.fr/les-decodeurs/article/2025/01/10/la-chute-de-dark-bank-le-banquier-du-crime-organisation-qui-ait-a-blanchir-plus-d-un-billion-euros_6490703_4355770.html
3. Stephen Katte (2025), "Crypto: 'Dark stablecoins' could emerge in the face of tighter regulations", *Cointelegraph,* May 2025, [accessed 11 June 2025], available at: https://en.cointelegraph.com/news/regulations-spark-censorship-resistant-dark-stablecoins
4. Anna Hirtenstein and Chen Aizhu (2025), "Russia leans on cryptocurrencies for oil trade, sources say", *Reuters,* March 2025, [accessed 11 June 2025], available at: www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/
5. Chainalysis (2025), "The Chainalysis 2025 Crypto Crime Report", [accessed 11 June 2025]. Format PDF. Available at: www.chainalysis.com/blog/2025-crypto-crime-report-introduction/
6. Timothy G. Massad (2025), "Stablecoins and National Security: Learning from Eurodollars", *Brookings.edu,* April 2025, [accessed 11 June 2025], available at: www.brookings.edu/articles/stablecoins-and-national-security-learning-the-lessons-of-eurodollars/
7. TRM Labs (2025), "2025 Crypto Crime Report. Key trends that shaped the illicit crypto market in 2024", [accessed 11 June 2025]. Format PDF. Available at www.trmlabs.com/resources/reports/2025-crypto-crime-report, accessed 10 June 2025.
8. Elliptic (2025), "The largest theft in history following the money trail from the Bybit Hack", *Elliptic Research,* February 2025, [accessed 11 June 2025], available at: www.elliptic.co/blog/bybit-hack-largest-in-history
9. Antoine Albertini (2025), "Removals in the cryptocurrency sector: a new wave of interpellations", *Le Monde,* May 2025, [accessed 11 June 2025], available at: www.lemonde.fr/societe/article/2025/05/27/nouvelle-vague-d-interpellations-dans-des-enquetes-sur-les-enlevements-du- secteur-des-cryptomonnaies_6608781_3224.html
10. United States Department of Justice (2024), "Foreign National Pleads Guilty to Laundering Millions in Proceeds from Cryptocurrency Investment Scams", November 2024, [accessed 11 June 2025], available at: www.

justice.gov/archives/opa/pr/foreign-national-pleads-guilty-laundering-millions-proceeds-cryptocurrency-investment-scams

11. TRM Labs (2025), "Bybit Piracy: Follow North Korea's greatest exploit", TRM *Blog. Prospects,* February 2025, [accessed 11 June 2025], available at: www.trmlabs.com/en/resources/blog/the-bybit-hack-following-north-koreas-largest-exploit
12. Aleksandar Tošić, Jernej Vičič and Niki Hrovatin (2025), "Beyond the surface: advanced wash-trading detection in decentralized NFT markets", *Finance Innov 11,* no. 86, February 2025, [accessed 11 June 2025], available at: https://rdcu.be/eqh6Q
13. Yuanzheng Niu et al. (2025), "Unveiling Wash Trading in Popular NFT Markets," *Cornell University,* March 2025, [accessed 11 June 2025], available at: www.arxiv.org/abs/2403.10361
14. Elliptic (2024), "North Korean hackers return to Tornado Cash despite sanctions", *Elliptic Research,* March 2024, [accessed 11 June 2025], available at: www.elliptic.co/blog/north-korean-hackers-return-to-tornado-cash-despite-sanctions
15. Benjamin H. Bratton (2016), "The Stack: On Software and Sovereignty", *MIT Press Direct,* February 2016, [accessed 11 June 2025], available at: www.direct.mit.edu/books/monograph/3504/The-StackOn-Software-and-Sovereignty
16. Challenges (2025), "North Korea: the 1.5-billion-dollar crypto-breaker that powers Pyongyang's war machine", *Challenges, April 2025,* [accessed 11 June 2025], available at: www.challenges.fr/la-verticale-cyber/coree-du-nord-le-casse-crypto-a-15-billion-qui-alimente-la-machine-de-guerre-de-pyongyang_601303
17. Greg Otto, "Russian crypto exchange Garantex seized in international law enforcement operation", *Cyberscoop, March 2025,* [accessed 11 June 2025], available at: www.cyberscoop.com/garantex-seized-secret-service-doj-russia-crypto-sanctions/

This publication was developed within the framework of the project on the "Development of French Financial Intelligence Unit's expertise focused on digital finance and virtual assets", co- funded by the European Union via the Technical Support Instrument, and implemented by the Council of Europe, in co-operation with the European Commission. As part of this initiative, the European Commission and the Council of Europe has supported the French Financial Intelligence Unit – Tracfin with strengthening the capacities and knowledge in the area of crypto-assets and decentralised digital finance, therefore also allowing to enhance the quality of Tracfin's strategic and operational analysis functions.

PREMS 088525

ENG

The member states of the European Union have decided to link together their know-how, resources and destinies. Together, they have built a zone of stability, democracy and sustainable development whilst maintaining cultural diversity, tolerance and individual freedoms. The European Union is committed to sharing its achievements and its values with countries and peoples beyond its borders.

http: //europa.eu

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

www.coe.int

Co-funded by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Co-funded and implemented by the Council of Europe