

Emerging money laundering and terrorist financing threats related to the use of decentralised finance



COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Emerging money laundering and terrorist financing threats related to the use of decentralised finance

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.

This document is for restricted, personal, and non-commercial use by the intended recipients only. Further distribution is not permitted.

The reproduction of extracts (up to 500 words) is authorised, except for commercial purposes, as long as the integrity of the text is preserved, the excerpt is not used out of context, does not provide incomplete information or does not otherwise mislead the reader as to the nature, scope or content of the text. The source text must always be acknowledged as follows: “© Council of Europe, year of the publication”. All other requests concerning the reproduction/translation of all or part of the document should be addressed to the Publications and Visual Identity Division, Council of Europe (F-67075 Strasbourg Cedex or publishing@coe.int).

All other correspondence concerning this document should be addressed to the Directorate General Human Rights and Rule of Law of the Council of Europe, Council of Europe, F-67075 Strasbourg Cedex, E-mail: contact.econcrime@coe.int.

Cover design and layout: Publications and Visual Identity Division (DPIV), Council of Europe

Cover photo: Shutterstock

This publication has not been copy-edited by the DPIV Editorial Unit to correct typographical and grammatical errors

© Council of Europe, December 2025
Printed at the Council of Europe

For further information please contact:

Directorate General Human Rights and Rule of Law – DG I
Directorate of Security, Integrity and Rule of Law
Economic Crime and Corruption Department
Economic Crime and Cooperation Division

Authors:

Jérôme COCHARD
and Yann LOUBRY
www.coe.int/econcrime

Contents

ABBREVIATIONS	5
1. EXECUTIVE SUMMARY	7
1.1. Scope	7
1.2. Content	7
1.3. Context	8
2. DECENTRALISED FINANCE – GENERAL OVERVIEW	9
2.1. Origins of the decentralised finance	9
2.2. Defi architecture	11
2.3. Smart contracts	12
2.4. Decentralised applications	13
2.5. Tokens	14
2.6. Governance	16
2.7. Use cases of DeFi	17
2.8. Stablecoins	18
2.9. DeFi vulnerabilities	19
2.10. DeFi regulatory framework	20
3. AN OVERVIEW OF EMERGING THREATS	23
3.1. The intersection of crime and Defi	23
3.2. Defi as an opportunity	24
3.3. DeFi as a target	29
3.4. Defi as a perpetrator	33
3.5. Defi as an intermediary	35
4. TOOLS AND RESOURCES FOR INVESTIGATIONS	39
4.1. Crypto analysis – step by step	39
4.2. Specifics of DeFi-related investigations and analysis	40
4.3. Smart contracts' analysis	41
4.4. Some useful tools and resources	44
5. LIMITATIONS AND CHALLENGES	53
5.1. A strengthened tough perfectible framework	53
5.2. Investigations made more complex	54
5.3. Expertise	57
5.4. Crypto-assets' recovery: freezing, seizing and managing	58
5.5. International cooperation	63
6. GOOD PRACTICES AND RECOMMENDATIONS	65
6.1. Regulatory framework	65
6.2. Continuous monitoring	65
6.3. Education and training	67
6.4. Investigating capacity	68
6.5. National cooperation	69
6.6. Asset seizure, recovery and management	70
6.7. International cooperation	70
6.8. Public-private cooperation	71

7. BIBLIOGRAPHY	73
7.1. Legal and Regulatory Texts	73
7.2. Institutional reports and publications	74
7.3. Academic and research	75
7.4. Press and news articles	76
7.5. Professional / Corporate / Technical Sources	76
8. LIST OF RESOURCES AND TOOLS	79
9. GLOSSARY	81

Abbreviations

AI	Artificial intelligence
AML/CFT	Anti-money laundering/countering the financing of terrorism
AMLA	Authority for Anti-Money Laundering and Countering the Financing of Terrorism
AMM	Automated market makers
API	Application programming interface
ARTs	Asset-referenced tokens
AWS	Amazon Web Service
BTC	Bitcoin
CaaS	Crimeware-as-a-service
CASP	Cryptoasset service provider
CA	Contract address
CeDeFi	Centralised Decentralised Finance
CeFi	Centralised Finance
CEX	Centralised Exchange
DaaS	Drainer-as-a-service
DAO	Decentralised autonomous organisation
dApps	Decentralised applications
DeFi	Decentralised Finance
DEX	Decentralised exchange
DNS	Domain Name System
EBA	European Banking Authority
ENS	Ethereum Name Service
EMARs	European mutual assistance requests
EMTs	Electronic money tokens
EOA	Externally owned account
ERC	Ethereum request for comment
ESMA	European Securities and Markets Authority
ETH	Ethereum
EU	European Union
EVM	Ethereum Virtual Machine
FATF	Financial Action Task Force
FIU	Financial intelligence unit

Genius Act	Guiding National Innovation for US Stablecoins Act
ICCRs	International criminal cooperation requests
ICO	Initial Coin Offering
IP	Internet Protocol
KYB	Know your business
KYC	Know your customer
LEA	Law enforcement agency
LP	Liquidity provider/ pool
MiCA	Markets in Crypto-Assets Regulation
ML	Money laundering
MOOCs	Massive open online courses
NRA	National risk assessment
NFT	Non-fungible token
OFAC	US Office of Foreign Assets Control
OSINT	Open source intelligence
OTC	Over-the-counter
P2P	Peer-to-peer
PABC	Party Ape Billionaire Club (NFT collection)
PIN	Personal identification number
QR	Quick-response
SIENA	Europol's Secure Information Exchange Network Application
TF	Terrorist financing
TFR	Transfer of Funds Regulation
TradFi	Traditional finance
TVL	Total Value Locked
UNODC	United Nations Office on Drugs and Crime
US	United States
VASP	Virtual asset service provider
VPN	Virtual private network

1. Executive Summary

1.1. Scope

This study is intended for members of law enforcement agencies (LEAs) and financial intelligence units (FIUs) in charge of combating financial crimes, money laundering and terrorist financing. It is aimed more specifically at those responsible for conducting investigations as well as operational and strategic analyses within these services.

The objective of this document is threefold:

- ▶ Provide a general understanding of decentralised finance (DeFi) and the associated money laundering and terrorist financing (ML/TF) risks;
- ▶ Present tools and resources that can be helpful from an operational perspective to analyse and investigate flows related to DeFi;
- ▶ Suggest ways of enhancing the effectiveness of analyses and investigations, through the identification of best practices and recommendations.

1.2. Content

The study addresses the following topics:

- ▶ A general description of the DeFi's role, regulatory framework, developments and challenges;
- ▶ A presentation of some typologies and emerging risks associated with decentralised finance;
- ▶ The identification of obstacles and limitations that may hinder the effectiveness of analyses and investigations in that field;
- ▶ A guidance on specific tools and resources that could facilitate the work of analysts and investigators;
- ▶ Proposals and recommendations for strengthening the effectiveness of investigative services, notably focusing on training, public-private partnerships, national and international cooperation.

1.3. Context

Inspired by libertarian ideals, the blockchain technology was originally developed to create a secure digital payment method free from any central or state control. The emergence of the Bitcoin blockchain in 2008 laid the foundation for an unprecedented transformation of the way the world transacts.

As bitcoin gained popularity, developers realised that blockchains could be used for much more than peer-to-peer electronic money. In 2015, Ethereum was introduced as a platform for programmable money, marking a turning point in the evolution of crypto-assets. With its smart contracts capabilities, Ethereum has driven innovation across many industries, from supply-chain management to gaming, and especially decentralised finance. DeFi has grown rapidly on the Ethereum blockchain enabling users to access financial services autonomously, without intermediaries. This trend has been further reinforced by the rise of new blockchains and innovative products.

However, the growing adoption of crypto-assets has also led to their misuse by malicious actors. Criminals quickly recognised the potential of this technology for illicit financing and money laundering. With the advent of DeFi, practices mostly confined to the cybercrime community have spread rapidly to a much larger population.

Confronted with unprecedented risks, legislators have sought to regulate this sector, particularly in the European Union (EU) and the United States (US). In the EU, the recent “Anti-Money Laundering (AML) Package¹” represents a major step towards harmonising the legal framework. It strengthens the monitoring of crypto transactions and establishes a regulator at the EU level – the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA)². These emerging regulations primarily target the crypto industry, by imposing new requirements on centralised exchanges, seen as mandatory crossing points between DeFi and traditional finance. Yet, in its very essence, DeFi remains largely outside the scope of these regulations, even though it presents significant risks of misuse for financial crime and money laundering.

This study aims therefore to explain the technologies underlying decentralised finance and outline their practical uses. To effectively counter the fraudulent exploitation of this financial innovation, law enforcement and investigative services need specialised training to understand the technology and the challenges it creates.

-
1. Council of the EU (2024), “Anti-money laundering: Council adopts package of rules”, May 2024, accessed 15 October 2025, available at: www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/#:~:text=a%20regulation%20establishing%20a%20new,was%20adopted%20in%20May%202023
 2. Regulation - EU - 2024/1620 - FR - EUR-Lex

2. Decentralised finance – general overview

Decentralised finance, or DeFi, is a generic term referring to all financial services that do not require the involvement of central institutions such as banks or states. DeFi is an alternative financial system that replicates traditional banking services using blockchain technology. It relies on smart contracts deployed on the blockchain. This system allows crypto-assets to be used autonomously, without having to go through centralised platforms controlled by third parties.

2.1. Origins of the decentralised finance

The first blockchain, Bitcoin, was designed primarily for the transfer of value (BTC). While it remains the leading blockchain in terms of market capitalisation and is renowned for its strong security, it suffers from limited scalability – the ability to handle a high volume of transactions swiftly and efficiently.

The “**Blockchain Trilemma**” suggests that blockchain systems face a trade-off between three key properties:

- ▶ decentralisation (cornerstone of this technology where control over the network is distributed among participants);
- ▶ security (capacity to prevent malicious entities from taking over); and
- ▶ scalability (capacity to handle a large number of transactions).

Improving one of these dimensions often comes at the expense of the others, prompting developers and researchers to continually seek innovative solutions that strike an optimal balance among the three.

To address this scalability issue, Ethereum Virtual Machine (EVM) type blockchains such as Ethereum have been developed. Unlike Bitcoin, they not only support transactions but also enable the execution of computer programmes such as smart contracts. This flexibility has significantly expanded the range of blockchain applications.

Following Ethereum’s success, new blockchains emerged with the aim of offering faster transactions, lower fees, greater scalability, and unique features. Some of the most notable examples include Avalanche (2021), Base (2023), Solana (2021), Polygon (2020), Arbitrum (2021), and Optimism (2021).

These developments have had several consequences:

- ▶ They expanded the number of use cases, applications and products, thereby accelerating DeFi adoption, particularly by reducing transaction fees.
- ▶ They encouraged the creation of bridges and aggregators to address liquidity fragmentation across different blockchains.

Staying true to the philosophy of blockchain's early pioneers, DeFi is defined in opposition to centralised finance (CeFi). CeFi refers to entities that provide individuals and companies with access to crypto-assets but do not grant them full control over their funds. By holding the corresponding private keys, these intermediaries retain ultimate control over their customers' assets.

Crypto-asset service providers (CASPs) are the main actors in CeFi. Functioning like "crypto banks", they enable clients to buy, sell and manage crypto-assets without dealing with the technical complexities of securing their funds. By also operating as exchange platforms for crypto/fiat conversions, CASPs play a crucial role in the broader crypto ecosystem.

Wallets, public keys versus private keys

A crypto wallet consists of two key components: a public key and a private key. The public key serves as the wallet's address and can be shared with third parties in order to receive funds. In certain cyberattack scenarios, malicious actors may provide victims with their own public key, leading victims to unknowingly transfer funds directly to the attacker's wallet.

The private key, on the other hand, must remain strictly confidential. It constitutes the cryptographic element that authorises and enables the execution of asset transfers.



Supporters of decentralised finance highlight the following benefits of this network:

- ▶ A non-custodial system, where participants hold and manage their private keys, and therefore their digital assets directly.
- ▶ A self-governed and community-driven network.
- ▶ A global and permissionless access, allowing anyone to participate, regardless of their locations (having a crypto wallet and an internet connection are the only requirements).

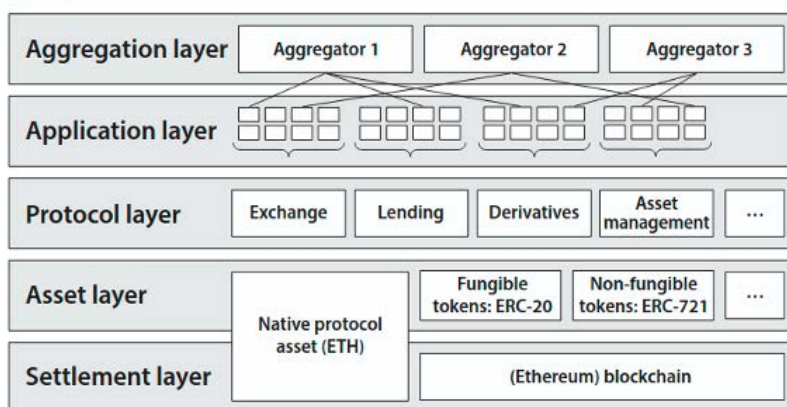
- ▶ Uninterrupted operations, without time constraints. Most DeFi protocols are open source and allow the community to review and further develop the code underlying the protocols. In terms of governance, the distribution of governance tokens in many DeFi applications allows users to participate in some decision-making related to the application, depending on the specific arrangements of each application.
- ▶ An enhanced transparency.
- ▶ An enhanced security guaranteed by the use of blockchain technology, which is resistant to fraud and manipulation. DeFi protocols can be designed in a way that prohibits intervention and manipulation.

Over the past few years, DeFi has experienced a significant growth, both in terms of innovations and of volume. Its activity, measured in Total Value Locked (TVL), is estimated at nearly 150 billion US dollars³.

2.2. Defi architecture

Blockchain layers are the structural components of a blockchain system, with each layer serving a distinct and specialised function.

The DeFi Stack



Source: Fabian Schär (2021), Decentralised Finance: on blockchain and smart contract-based financial market⁴

Layer 1 or settlement layer consists of the blockchain itself along with its native protocol asset (e.g. bitcoin (BTC) on the Bitcoin blockchain and other (e.g. ETH on the Ethereum blockchain). It records ownership securely and ensures that all changes comply with the system's rules.

3. Source: DefiLlama - DeFi Dashboard, accessed 29 September 2025.

4. Schär F. (2021), "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets", Federal Reserve Bank of St. Louis Review, Second Quarter 2021, accessed 6 October 2025, format PDF, available at: www.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

Layer 2 or **asset layer** includes all assets built on top of the settlement layer. It covers both the native protocol assets and any additional tokens created on the blockchain (e.g. USDC or Non-fungible tokens (NFTs) on the Ethereum blockchain). Each blockchain defines its own rules for token issuance, codified in standards such as ERC-721 for NFTs on Ethereum, SPL for Solana, or BEP-20 for Binance Smart Chain.

Layer 2 is also a collective term used to describe blockchain scaling solutions designed to enhance the performance of primary blockchains. These solutions add value by enabling faster and lower-cost transactions.

- ▶ **Lightning network:** Enables off-chain transactions through a network of payment channels, significantly increasing transaction speed (primarily for Bitcoin).
- ▶ **Zero-knowledge (zk) rollups and optimistic rollups:** Bundle hundreds of transactions into a single transaction on Layer 1. The transactions are executed off-chain, while the resulting data is stored on the blockchain. Examples include Optimism and Arbitrum.

However, many Layer 2 chains are not yet supported by most commercial blockchain investigation tools, which presents challenges for investigators.

Layer 3 or **protocol layer** defines rules or standards that govern a specific task or activity (such as decentralised exchanges (DEXs) or lending markets). These standards are typically implemented through smart contracts that can be accessed by users and DeFi applications.

Layer 4 or **application layer** consists of user-oriented applications that interact with protocols. The decentralised applications (dApps) are web-based front ends that make an easier use of protocols, by abstracting the smart contract interaction.

Layer 5 or **aggregation layer** is an extension of the application layer. Aggregators create user-centric platforms that connect to several applications and protocols, and usually provide tools to compare services, allow users to perform otherwise complex tasks by connecting to several protocols simultaneously, and combine relevant information in a clear and concise manner.

2.3. Smart contracts

Smart contracts are a cornerstone of the DeFi ecosystem with Ethereum being a pioneer of such technology and decentralised applications. A smart contract is an application or software that executes automatically when the predefined conditions written in its code are met, following an "IF/WHEN... THEN..." logic. Stored on a blockchain, the code ensures that the contract's terms are fulfilled before it is triggering any action, with execution carried out by a decentralised network of validators.

A good example can be drawn from the insurance industry. Imagine a rule stating that any train delay exceeding two hours entitles passengers to 100 euros of compensation:

"IF train delay > 2 hours, THEN compensation = 100 euros"

Traditionally, the affected passenger would file a claim with the train operator or insurance company, which would then process the file, verify that the damage was real and covered, and – if approved – initiate the payment.

With a smart contract, this process can be fully automated. The delay event would be detected by a trusted service known as an oracle⁵, which feeds external data into the blockchain. The smart contract then automatically verifies the claim, ensuring that the event occurred, the terms are met, and all predefined conditions are satisfied. If everything checks out, the contract executes the payout without further human intervention.

The responsibility for verifying compliance with these rules lies with validators – specialised blockchain nodes⁶ that confirm transactions and maintain the integrity of the network.

In addition to their decentralised nature, smart contracts are defined by the following attributes:

- ▶ **Determinism:** A smart contract will always produce the same output when given the same input.
- ▶ **Transparency:** On public blockchains, smart contract code is open source and visible to everyone. All transactions and state changes are publicly auditable, making them valuable assets for investigators.
- ▶ **Immutability:** Once a smart contract is deployed to the blockchain, its code cannot be changed or reversed. This provides a high degree of certainty regarding its future execution.
- ▶ **Censorship resistance:** Once deployed, a smart contract is unstoppable – no entity, including governments or regulators, can prevent it from running or interacting with users.

By eliminating the need for intermediaries such as banks or brokers, smart contracts streamline transactions, saving both time and cost.

2.4. Decentralised applications

Decentralised finance is developing mainly through decentralised applications, or dApps. Those are similar to their massively used counterparts on connected devices (which grant access to social networks, bank accounts, or the purchase of goods and services). However, while the latter are developed and owned by private companies, which manage their customers' data on their servers, dApps operate on a peer-to-peer (P2P) network or blockchain, without intermediation.

5. An oracle is a trusted service that operates as a bridge between the blockchain and the real world. It sends a signal, which causes the launch of the smart contract. In this example, the oracle checks the train data and sends a message ("train delayed by 2 hours"), meaning that the IF condition is fulfilled.

6. A node is a computer connected to a blockchain network, who stores a copy of this blockchain; a validator is a special node who is checking and approving the transactions (or actions).

First emerging in 2016 on Ethereum, dApps have gradually developed on other blockchains such as Solana, BSC and Polygon (which are more efficient in terms of scalability, cost and speed). Today, their number is reported to be over 17 000⁷.

Available in various sectors (infrastructure, social networks, and other), dApps have particularly invested in the field of finance:

- ▶ Financial dApps offer the possibility of carrying out transactions such as asset conversion (Uniswap), staking (Lido), lending and borrowing (AAVE);
- ▶ Gaming dApps are those developed in connection with online games, which allow users to earn and hold tokens (Axie Infinity, World of Dypians⁸);
- ▶ dApps dedicated to NFTs are specifically designed to manage, trade and showcase NFTs, which became popular from 2021.

2.5. Tokens

Ether: Ether is the native token of the Ethereum blockchain. It can be subdivided into smaller units called “wei” (1 ETH = 10¹⁸ wei).

- ▶ While often used as a currency and speculative asset (despite not being designed for this purpose), Ether’s primary role is to power applications running on the Ethereum network.
- ▶ This function is referred to as “gas”: every transaction requires a specific amount of gas to be executed, which is paid in ETH.

Variety of tokens: Tokens extend the functionality of blockchains beyond native assets. They are used to:

- ▶ Provide access to decentralised applications;
- ▶ Allocate governance rights within decentralised organisations (DAOs);
- ▶ Certify unique ownership through non-fungible tokens.

These diverse uses highlight tokens’ central role in DeFi and underscore the importance of standardised frameworks to ensure interoperability and security across blockchain networks.

Major token standards: Empirical data suggests that more than 90% of crypto-assets in circulation rely on a few dominant token standards, including:

Standard	Description
ERC-20	ERC-20 is the most widely used standard on Ethereum governing fungible tokens. It specifies essential functions such as token transfers, balance checks, and third-party spending approvals. ERC-20 tokens formed the backbone of many Initial Coin Offerings (ICOs). Studies estimate that around 75% of all fungible tokens across public blockchains are ERC-20 or ERC-20 derivatives.

7. Source: [Top Blockchain Dapps | DappRadar](#), accessed 25 September 2025.
8. See: [World of Dypians](#)

ERC-721	A standard for non-fungible tokens, which are unique and indivisible. It enables the representation of distinct digital assets such as artworks, in-game items, or ownership certificates.
ERC-1155	A hybrid standard that supports both fungible and non-fungible tokens within a single smart contract. It reduces gas costs and allows batch transfers, making it particularly suited to blockchain gaming and metaverse applications. ERC-1155 now accounts for an estimated 10–15% of new NFT issuances ⁹ .
TRC-20	The Tron blockchain's equivalent of ERC-20. It ensures compatibility with Tron smart contracts and dApps and is widely used for stablecoins such as USDT (Tether). As of 2025, more than 50% of Tether's circulating supply is issued as TRC-20, making Tron one of the highest-volume blockchains ¹⁰ .
BEP-20	A token standard modelled on ERC-20 but specific to Binance Smart Chain (BSC). It enables token creation within Binance's ecosystem, particularly for DeFi applications. BSC accounts for roughly 20% of DeFi-related token activity ¹¹ .
SPL	The native token standard of the Solana blockchain, designed for high-speed and low-cost transactions. It supports both fungible tokens and NFTs. Solana NFTs (SPL-based) consistently rank second only to Ethereum in trading volume, representing billions of dollars in cumulative transactions.
Algorand ASA	The Algorand Standard Asset framework enables the issuance of diverse digital assets, including fungible tokens, NFTs, and stablecoins. It offers advanced features such as freezing, revocation, and address restrictions, providing additional flexibility.

Token functions beyond currency include:

- ▶ *Utility*: Grant holders' access to products or services, such as decentralised storage.
- ▶ *Governance*: Represents voting rights within DAOs or even formal legal systems.
- ▶ *Collectibles*: Serves as proof of ownership of digital collectibles (e.g. CryptoPunks) or physical assets (e.g. a painting).
- ▶ *Identity*: Represents a digital identity (e.g. an avatar) or a legal identity (e.g. a national ID).
- ▶ *Attestation*: Functions as a certification or proof of fact, issued either by an authority or through a decentralised reputation system (e.g. land ownership records, birth certificates).
- ▶ *Asset representation*: Represents ownership of intrinsic or extrinsic, tangible or intangible assets (e.g. gold, real estate, or energy).

9. Nansen (2022), "Nansen adds ERC1155 support for NFTs", February 2022, accessed 15 October 2025, available at: www.nansen.ai/post/nansen-adds-erc1155-support-for-nfts

10. See: [TRC20 USDT Supply Reaches Record High in 2025 | Binance News on Binance Square](#), accessed 13 October 2025.

11. See: [All Chains DeFi TVL - DefiLlama](#), accessed 13 October 2025.

2.6. Governance

Protocols are typically developed and maintained by organisations, often structured as DAOs. These entities consist of governance token holders, whose distribution allows users to participate in decision-making related to the protocol's development and operations. The number of DAOs is currently estimated at over 50 000¹².

However, decentralisation in DeFi is not absolute. The degree of decentralisation varies across protocols and directly affects how potential regulations could be applied.

- ▶ *Fully decentralised protocols* most closely embody the original vision of DeFi. Once launched, they cannot be stopped, making direct legislative action difficult to implement. While banning or shutting them down is virtually impossible, regulators can still target front-end operators and fiat on/off-ramps (e.g. exchanges and custodians).

A notable example is Tornado Cash, a crypto-asset mixing service based on smart contracts. Despite its addresses being sanctioned by the US Office of Foreign Assets Control (OFAC)¹³ in August 2022 for alleged involvement in money laundering, the underlying smart contract remains functional and can still be used. This marked the first time a non-custodial crypto-asset smart contract was sanctioned, setting an important precedent and demonstrating that Ethereum is not entirely immune to censorship or cooperation.

- ▶ The term DeFi also encompasses *entities that are not fully decentralised*, sometimes referred to as CeDeFi. In such cases, decentralisation is often more nominal than real:
 - A small number of governance token holders may wield dominant influence or even collude to take over a project.
 - Developers may retain effective control over the codebase.
 - Human intervention is always present at some stage – whether in development, maintenance, or promotion.

The critical issue is the ability to identify individuals or groups with sufficient control who can be held accountable. This reflects the Financial Action Task Force (FATF) approach, as outlined in [section 5.1](#).

An example of the hybrid nature of DeFi is the Finnish company Tesseract, a managed yield provider. While operating in the DeFi sector, its management chose to apply for a license¹⁴ under the Markets in Crypto-Assets (MiCA) Regulation¹⁵, illustrating the overlap between decentralised practices and traditional regulatory compliance.

12. See: [DeepDAO – Discovery Engine for DAO Ecosystem](#), accessed 13 September 2025.

13. OFAC is the agency within the US Department of Treasury responsible for maintaining and enforcing the US sanctions policy.

14. Omelchenko D. (2025), "Managed DeFi Yield Provider Tesseract Secures MiCA License", *The Defiant*, September 2025, accessed 6 October 2025, available at: <https://thedefiant.io/news/defi/defi-yield-provider-tesseract-mica-license>

15. [Regulation - 2023/1114 - FR - EUR-Lex](#)

2.7. Use cases of DeFi

Decentralised finance primarily offers a wide range of products and services, which often replicate those offered by the traditional financial sector, but under different conditions. The most common uses include savings, loans, investments, insurance, token exchanges, and other.

Service	Service providers/ examples	Description
Swapping	Uniswap, PancakeSwap	Crypto trading without an intermediary, using smart contracts
Lending and borrowing	AAVE, Compound, Maker DAO, Blur Lending, JustLend	Lend to earn interest, borrow against collateral
Yield Farming and Liquidity Mining	Yearn Finance, Curve	Earn rewards by providing liquidity or participating in DeFi activities
Staking	Lido, Kiln	Lock crypto to support networks and earn rewards / interests
Cross chain bridges	RenBridge, ThorChain, Across, Stargate	Transfer crypto-assets to another blockchain
NFT Marketplace	Opensea, Rarible, BlurBids, ImmutableX	Create, buy, sell, and auction NFTs
Derivatives and synthetic assets	Syntheticx, dYdX, Drift Trade, Jupiter Perpetual Exchange	Sophisticated speculative instrument: – tokens that replicate the value of real-world assets = synthetic assets – contracts whose value depends on the price of an underlying asset (e.g. futures, options, commodity...) = derivatives
Stablecoins	Circle (USDC), Tether (USDT), DAO Maker (DAI)	Emission of crypto-assets pegged to a fiat currency to reduce volatility
Mixing	Tornado Cash, Railgun	Anonymise transactions by pooling and redistributing funds, making it difficult to trace the original source or destination
Insurance	Nexus Mutual	Protection against risks, such attacks or thefts
Asset management	DeBank, Yearn Finance	Tools to manage and optimise DeFi investments
Oracles	Chainlink, Pyth Network	Provision of off-chain information

DeFi very often replicates traditional finance opportunities, as illustrated below.

Crypto lending and borrowing were one of the earliest – and remain one of the most popular – DeFi applications. The concept is similar to commercial bank deposits and loans, but without a central authority to decide who can deposit, borrow, or under what terms. Anyone can lend their assets and earn interest or borrow crypto-assets against deposited collateral.

Flash loans

Flash loans are a uniquely DeFi innovation with no equivalent in traditional finance. They allow users to borrow assets without posting collateral, on the condition that the loan (plus interest) is repaid within the same block. Skilled traders often use flash loans to exploit arbitrage opportunities – profiting from temporary price differences across markets.

However, flash loans also have a darker side. In a flash loan attack, malicious actors combine flash loans with other vulnerabilities to manipulate market prices and extract significant profits.

Staking involves locking up crypto-assets to participate in validating transactions, earning rewards in return.

Restaking builds on this concept by allowing assets that are already staked to be staked again, thereby generating supplementary rewards.

Yield farming is a strategy aimed at maximising returns by moving capital across different DeFi protocols¹⁶ and derivatives¹⁷. It is essentially an advanced trading technique adapted to the DeFi environment, which involves higher rewards but also greater risks.

2.8. Stablecoins

Stablecoins are digital assets designed to maintain a stable value by pegging themselves to a reference asset, most often a fiat currency such as the US dollar or the euro. Their primary advantage is reducing the volatility of crypto-assets, making them useful as both a medium of exchange and a store of value.

Stablecoins are commonly used as on- and off-ramps to crypto-assets, serving as vehicles for speculative investments. Increasingly, they are also employed as instruments for cross-border payments. They are particularly valuable where domestic financial systems are weak or costly to use, or where international financial transactions are restricted due to capital controls or externally imposed sanctions.

There are three distinct types of stablecoins, whose characteristics have direct regulatory implications:

- ▶ *Centralised stablecoins* are issued by companies and backed by reserves of fiat currency held off-chain by the issuer. The two largest examples are USDC

16. See details here: <https://finematics.com/yield-farming-explained/>

17. See details here: <https://finematics.com/derivatives-in-defi-explained/>

and USDT, issued respectively by Circle and Tether, together representing over 90% of the market¹⁸.

- ▶ *Decentralised stablecoins* are governed by smart contracts and DAOs and collateralised by other crypto-assets on-chain¹⁹. They are decentralised in that no single entity controls the reserves. DAI, issued by MakerDAO, is the leading example.
- ▶ *Algorithmic stablecoins* (e.g. the former TerraUSD) are governed by algorithms that automatically adjust token supply to maintain their peg. However, they are vulnerable to depegging risks and have proven largely ineffective, which explains their limited use within the market.

Issuers of centralised stablecoins are regulated entities (see section 2.10) and retain control over their assets, with the ability to freeze, seize, blacklist, or revoke tokens. In contrast, decentralised stablecoins cannot be seized due to the absence of a central authority.

The total market capitalisation of stablecoins has surpassed 293 billion US dollars, with USDT (172 billion US dollars) and USDC (73 billion US dollars²⁰) together accounting for around 83% of the market.

Stablecoins have become a pivotal use case in digital asset markets, serving both legitimate and illicit purposes. According to a recent report, they account for nearly two-thirds of illicit transactions²¹.

Their growing use illustrates the paradox of DeFi. On one hand, stablecoins promote DeFi adoption and strengthen its interconnection with CeFi and traditional finance (TradFi), creating new opportunities for users. On the other, they represent one of the most significant vulnerabilities of the DeFi ecosystem.

2.9. DeFi vulnerabilities

The growth of DeFi, that undergoes constant changes in a still largely unregulated sector, is raising concerns in terms of consumer protection, financial stability and the possible misuse of its applications for criminal purposes. Several specific risks have been identified in connection to DeFi, including:

- ▶ vulnerabilities of smart contracts;
- ▶ governance and control issues in organisations managing protocols;
- ▶ price manipulation and extreme volatility;
- ▶ misuse of DeFi for criminal purposes, particularly tax fraud, money laundering, terrorist financing and sanctions evasion.

Some of these risks are further described in [Chapter 3](#).

18. Dune and Artemis (2025), “*The State of Stablecoins 2025: Supply, Adoption & Market Trends*”, accessed 3 October 2025, format PDF, available at: <https://dune.com/stablecoin-download>

19. Since this collateral can be volatile, these stablecoins are often over-collateralised.

20. See: [Stablecoins Circulating - DefiLlama](#), accessed 23 September 2025.

21. Chainalysis (2025), “*The Chainalysis 2025 Crypto Crime Report*”, accessed 6 October 2025, format PDF, available at: www.chainalysis.com/blog/2025-crypto-crime-report-introduction/

2.10. DeFi regulatory framework

DeFi remains largely outside the scope of regulation, which has so far focused primarily on centralised players and intermediaries. However, significant regulatory initiatives targeting this sector are likely in the coming years. The key challenge lies in determining jurisdiction and identifying the natural or legal persons who may be held liable within protocols that operate without a central authority.

2.10.1. Europe

Coming into force in December 2024, the Markets in Crypto-Assets Regulation²² was adopted to regulate the crypto-asset market in the European Union. Together with Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (the Transfer of Funds Regulation, TFR)²³ and the AML package²⁴, this framework imposes obligations on crypto-asset service providers similar to those applicable in the traditional financial sector. These include customer and business identification, transaction monitoring under the “travel rule”, enhanced due diligence for self-hosted wallets and harmonised supervision at European level through the creation of a unified regulator (AMLA).

DeFi activities do not appear to fall within this framework, with services provided in a “fully decentralised manner” explicitly excluded from its scope²⁵. However, debate persists over whether certain entities, such as DAOs, should be brought under MiCA insofar as they may not be entirely decentralised²⁶.

Stablecoins are the notable exception. Under MiCA, both asset-referenced tokens (ARTs) and electronic money tokens (EMTs) are subject to prudential standards, governance requirements, and marketing restrictions:

- ▶ *Asset-referenced token*: A cryptographic token used for exchange, whose value can be pegged to multiple reference assets (fiat currencies, commodities, or other crypto-assets, or a mix). To date, no ART issuer (i.e. non-fiat-backed stablecoin) has been authorised.
- ▶ *Electronic money token*: A cryptographic token used for exchange that is pegged to a single fiat currency (e.g. USDT, USDC). EMT issuers must operate as electronic money institutions (EMIs) but on distributed ledger technology.

EMT issuers and providers are subject to specific obligations, including:

22. Regulation - 2023/1114 - EN - EUR-Lex

23. Regulation - 2023/1113 - EN - EUR-Lex

24. Consisting of the following:

- Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- Directive (EU) 2024/1640 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- Regulation (EU) 2024/1620 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism.

25. See Recital 22 of MiCA Regulation 2023/114: “Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation”.

26. Latka N. (2024), “Is DeFi Truly Exempt from MiCA Regulations?”, *Merkle Science*, June 2024, accessed 16 September 2025, available at: www.merklescience.com/blog/is-defi-truly-exempt-from-mica-regulations

- ▶ supervision and regulation of all EMTs by the European Banking Authority (EBA);
- ▶ the requirement to obtain both an e-money institution licence (under the Electronic Money Directive²⁷) and a MiCA licence to issue EMTs legally.

Since 30 June 2024, the provision of crypto-asset services related to non-compliant ARTs and EMTs is prohibited, as MiCA regulation requires non-compliant stablecoins to be delisted by CASPs.

As of 25 September 2025, eleven EMT issuers have been authorised. It is interesting to note that Tether is excluded, as it has not obtained an EMI licence and does not meet reserve requirements.

Finally, European Securities and Markets Authority (ESMA) and EBA have been tasked with monitoring DeFi developments and reporting to the European Commission, which is expected to propose further regulatory measures.

2.10.2. United States

In the United States, the legal framework consists of both federal laws and state-specific regulations, some of which are broader or more permissive than others.

In July 2025, the Guiding National Innovation for US Stablecoins Act (known as the Genius Act)²⁸ was adopted at the federal level. The Act seeks to define and regulate the stablecoin sector, aiming simultaneously at promoting innovation and ensuring the protection of the financial system and consumers.

The main provisions of the Genius Act include:

- ▶ the definition of “payment stablecoins”;
- ▶ the classification of stablecoin issuers, such as Circle or Tether, as financial institutions;
- ▶ the establishment of a single regulatory framework, imposing obligations such as mandatory liquidity reserves, regular audits and strict anti-money laundering and countering financing of terrorism (AML/CFT) requirements.

By providing a unified regulatory framework across the country, this regulation may be seen as a precursor to a more comprehensive and global regulation of DeFi activities in the near future.

2.10.3. Other jurisdictions

Awareness is growing globally of the challenges posed by the intertwining of DeFi with traditional finance, along with the associated risks, as reflected in several initiatives:

- ▶ In 2021, the FATF’s “*Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*”²⁹, noted that “creators, owners and operators or certain other persons who retain control or sufficient influence in

27. Directive - 2009/110 - FR - EUR-Lex

28. Text - S.1582 - 119th Congress (2025-2026): GENIUS Act | Congress.gov | Library of Congress

29. FATF (2021), “*Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*”, October 2021, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

DeFi arrangements' may be considered as CASPs". In June 2023, in its "*Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*", the organisation recommended that member states assess the risks associated with DeFi³⁰.

- ▶ In May 2025, Hong Kong adopted the Stablecoin Ordinance which regulates stablecoins pegged to the Hong Kong dollar. Issuers are required to obtain a licence from the national Monetary Authority and comply with strict obligations, including AML/CFT measures, regular audits and disclosure requirements.
- ▶ Some jurisdictions – such as Switzerland and Germany, as well as certain US states (e.g. Wyoming, Vermont) – have decided to grant legal personality to DAOs, thereby recognising *de facto* the centralised nature of these organisations.

30. FATF (2023), "*Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*", June 2023, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

3. An overview of emerging threats

With its (false) promise of anonymity, blockchain technology carried a risk of misuse, and crypto-assets were rapidly exploited by criminal actors, as shown in a growing number of financial crime investigations³¹.

3.1. The intersection of crime and DeFi

The shift in criminal activity caused by the development of the crypto ecosystem is twofold:

- ▶ On the one hand, crypto-assets are increasingly used to commit crimes and launder money as they enable borderless, instant and large-value transfers.
- ▶ On the other hand, DeFi has lowered the entry barrier and enabled new types of malicious actors. With minimal technical knowledge, individuals can now carry out cyber-attacks, defraud users, or launder funds from their homes.

Fraudulent uses of crypto-assets have expanded beyond traditional cybercrime and are closely linked to widely accessible technological tools:

- ▶ Criminals rely on specialised online and secure networks – such as Telegram channels or darknet forums – to share expertise and buy or sell illicit goods and services. These marketplaces offer guidance on criminal and money laundering techniques, anonymisation methods, phishing kits, malware for stealing private keys and wallet credentials, and stolen data (bank details, identity documents)³².
- ▶ Malicious actors increasingly leverage generative artificial intelligence (AI) to automate operations at scale. AI can be used to generate synthetic IDs, create automated crypto-asset accounts, run mass phishing campaigns, spin up multiple intermediary addresses (peeling chains), or identify high-value targets ahead of ransomware encryption.

DeFi amplifies these trends by enabling more sophisticated criminal techniques and new products that facilitate rapid and often anonymous transactions. As centralised exchanges face tighter regulation, criminals have migrated toward unregulated and anonymous alternatives to process illicit crypto-assets.

31. Chipolina S. (2023), "Cryptocurrencies play 'endemic role' in organised crime", *Financial Times*, October 2023, accessed 6 October 2025, available at: www.ft.com/content/378a05ac-a12b-41f9-a80c-fc79a36bc44b

32. Patairya D. K. (2023), "Crimeware-as-a-service: A new threat to crypto users", *Cointelegraph*, January 2025, October 2023, accessed 6 October 2025, available at: <https://cointelegraph.com/explained/crimeware-as-a-service-a-new-threat-to-crypto-users>

DeFi complicates investigations and prosecutions by allowing illicit flows to be fragmented across multiple, often automated protocols within an evolving legal framework.

Risk related to the use of decentralised finance can be classified into four main categories³³:

- ▶ *DeFi as an opportunity*: DeFi provides additional tools and techniques which can be misused for money laundering purposes.
- ▶ *DeFi as a target*: Protocols and services are directly targeted through exploitation of contract vulnerabilities and hacks – this accounts for around half of reported DeFi-related crimes.
- ▶ *DeFi as a perpetrator*: Cases in which DeFi actors actively participate in committing crimes.
- ▶ *DeFi as an intermediary*: Situations where DeFi actors are used by attackers to reach or exploit users.

3.2. Defi as an opportunity

DeFi can be used to transfer and launder the illicit proceeds of crime, offering techniques and services that extend beyond traditional money laundering schemes. It plays a major role in the layering phase³⁴ by providing mechanisms such as swaps (exchanging one crypto-asset for another), cross-chain bridges (moving assets between blockchains), mixers and liquidity pools. These tools may be used individually or in combination.

The sophistication of laundering schemes depends on the user's technical expertise and familiarity with crypto-assets and DeFi services. Nevertheless, law enforcement agencies have observed even low-skilled actors employing some of the techniques described above.

3.2.1. Obfuscation techniques

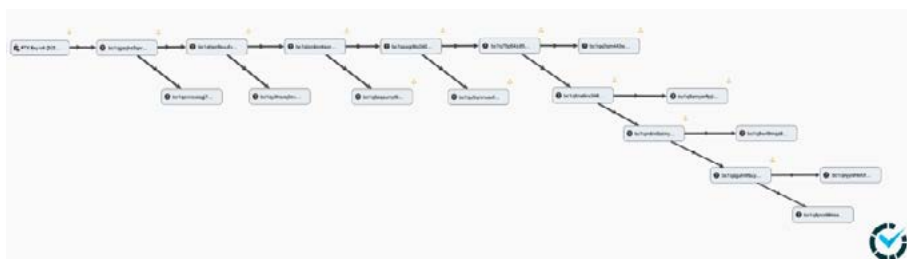
3.2.1.1. Traditional methods

Peeling chains: This method involves transferring small amounts of crypto-assets through multiple newly created addresses, making illicit transactions harder to trace.

After a large deposit (e.g. a ransomware payment in Bitcoin) enters a criminal-controlled wallet, small fractions are repeatedly moved to new wallets until the original balance reaches zero. The funds can then be sent to non-custodial addresses, exchanges, or mixers. Automated scripts and bots can execute peeling chains at high speed, generating hundreds of wallets in minutes, often outpacing manual investigations.

33. This distribution is inspired by the classification proposed in the following article: Carpentier-Desjardins C. et al. (2025), "Mapping the DeFi crime landscape: an evidence-based picture", *Journal of Cybersecurity*, Volume 11, Issue 1, 2025, Cornell University, January 2025, accessed 6 October 2025, available at: <https://arxiv.org/abs/2310.04356>

34. Along with placement and integration, layering is one of the three steps of the common ML classification. It consists in carrying out multiple and complex transactions in order to hide the illegal source of the funds.



Representation of a peeling chain linked to the FTX hack (Source: Scorechain³⁵)

Money mules: Similar in purpose, money mules are individuals – either unwitting or complicit – who transfer illicit funds for criminal organisations³⁶. They are often used in off-ramp operations, leveraging CASP custodial wallets as transit accounts, either temporarily or through purchased older accounts, to evade compliance detection.

In both cases, the aim is to obscure the origin of funds by multiplying transactions, making fraudulent patterns more difficult to detect for both reporting entities and law enforcement.

Gambling: Casinos and betting sites, particularly underregulated online platforms, remain popular for laundering funds³⁷. Without customer identification requirements, these platforms allow criminals to deposit tainted assets, co-mingle them with legitimate funds, and later withdraw them appearing as gambling winnings.

Case Example: Stake.com

Stake.com is an online crypto casino and sports betting platform operated by Medium Rare N.V., incorporated in Curaçao. It is one of the largest operators in the crypto-assets gambling sector.

Based in a jurisdiction often viewed as a haven for offshore casinos – where the regulator has limited or no power to enforce rules extraterritorially – *Stake.com* can readily evade local restrictions and operate in countries where it is banned. The simple use of a virtual private network (VPN) is often sufficient to bypass geoblocking.

Because no identity verification is required to open an account, *Stake.com* raises concerns about potential money laundering. Anyone can deposit tainted crypto-assets without placing bets, then withdraw the funds and present them as gambling winnings, giving the proceeds a seemingly legitimate (if not lawful) appearance.

35. See: [Scorechain investigates the FTX hack - Scorechain | Blockchain & Digital Assets Compliance](#)

36. See here for an example of networks being dismantled: Europol (2024), “*Crackdown on money mule service providers laundering over EUR 10 million*”, May 2024, accessed 6 October 2025, available at: www.europol.europa.eu/media-press/newsroom/news/crackdown-money-mule-service-providers-laundering-over-eur-10-million

37. UNODC (2024), “*Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*”, January 2024, accessed 6 October 2025, available at: www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html

3.2.1.2. Anonymity-enhancing tools and assets: mixers and privacy coins

Privacy coins: These crypto-assets have been designed to enhance user privacy and transaction anonymity. Unlike traditional crypto-assets, they obscure transaction details through cryptographic techniques, making them difficult to trace. Monero is the most prominent example due to its robustness. Although delisted by most CASPs, it remains available on less-regulated exchanges. As of September 2025, Monero ranked 26 by market capitalisation (~four billion US dollars³⁸) and is frequently used for darknet market transactions, ransomware payments, and, more recently, terrorist financing³⁹.

Mixers: These are services or protocols that obscure the origin and destination of crypto-assets by pooling funds from multiple users and redistributing them to prevent linking deposits with withdrawals. They can be classified into three categories:

- ▶ **Custodial mixers:** Centralised services that temporarily hold users' funds. They are less common due to risks such as theft or seizure by authorities.
- ▶ **Non-custodial mixers:** Users retain control of their funds while the service mixes them using protocols like CoinJoin (e.g. Wasabi, Samourai). Transactions are nearly untraceable if users follow best practices, although authorities can access data when platforms are shut down, as seen with ChipMixer in 2023⁴⁰.
- ▶ **Smart contract mixers:** Deployed directly on blockchains (e.g. Tornado Cash, Railgun) and using cryptographic techniques such as zero-knowledge proofs to unlink deposits from withdrawals. Users send their funds into the contract and then get their funds back from a new address. Due to smart contract immutability, these mixers remain operational even if blacklisted, as shown by the Tornado Cash example.

3.2.1.3. Cross-chain

The ability to swap crypto-assets between different tokens and blockchains is a routine service offered by many exchanges. While most swaps are legitimate, criminals have quickly adopted these techniques.

These transfers can be carried out in three ways:

- ▶ **Decentralised exchanges:** they allow conversions on the same blockchain (e.g. Uniswap⁴¹).
- ▶ **Bridges:** DeFi protocols enable transfers from one blockchain to another (e.g. 1inch⁴²).
- ▶ **Coin-swap services** (instant-swap exchanges): centralised services let users swap between assets or blockchains, often anonymously, via bespoke websites or Telegram channels (e.g. StealthEx).

38. See: <https://coinmarketcap.com>, accessed 25 September 2025

39. Roul A. (2024), "The Rise of Monero: ISKP's Preferred Cryptocurrency for Terror Financing", Global Network on extremism and technology, October 2024, accessed 6 October 2025, available at: <https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/>

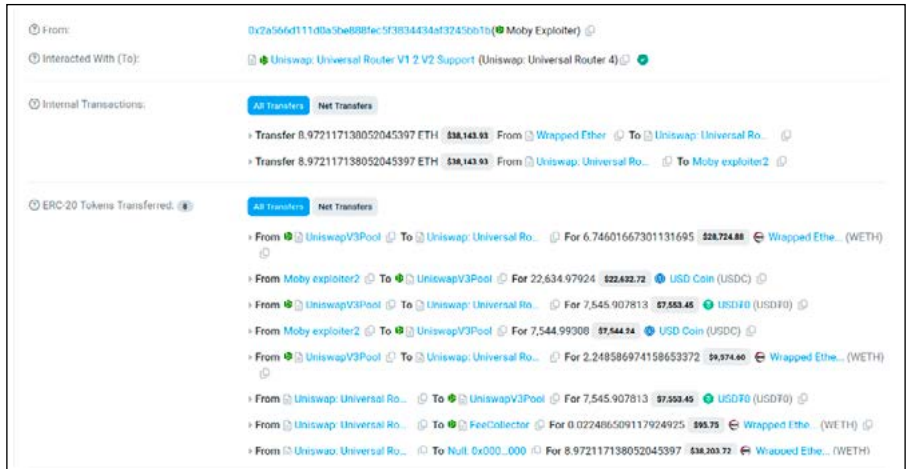
40. Europol (2023), "One of the darkweb's largest cryptocurrency laundromats washed out", March 2023, accessed 6 October 2025, available at: www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out

41. See: <https://app.uniswap.org/>

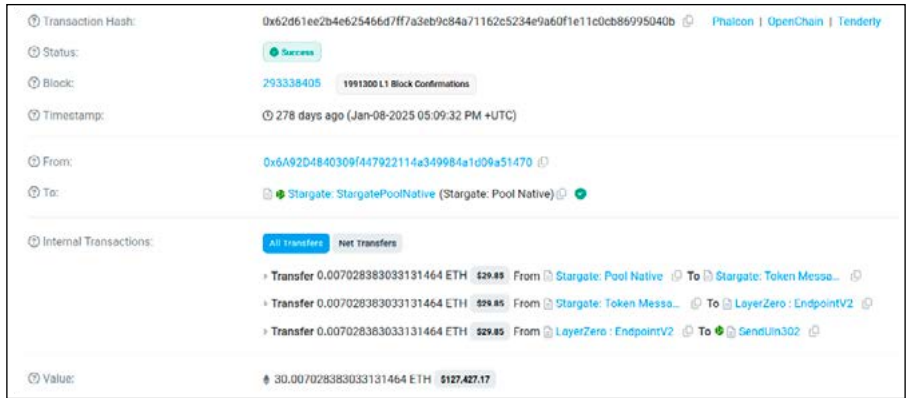
42. See: <https://1inch.io/>

With stronger AML/Know Your Customer (KYC) rules applied to traditional exchanges, laundering across blockchains has become particularly attractive for criminals, as illustrated by the RenBridge case⁴³.

Cross-chain activity complicates investigations. On a single chain, an investigator can analyse a DEX contract to see what tokens were swapped and where they went. In chain-hopping scenarios, investigators must trace funds through the bridge and then follow them on the destination blockchain to locate the transaction outputs. While this tracing is often feasible on major blockchains – especially with commercial analytics tools – it becomes much harder on less common chains.



A detailed view of a transaction showing a USDC > ETH swap linked to the Moby Trade exploit (Source: Arbscan.io, consulted in January 2025⁴⁴)



A detailed view of a subsequent cross-chain transaction leveraging Stargate Protocol (Source: Arbscan.io, consulted in January 2025⁴⁵)

43. Robertson A. (2022), "Hackers and fraudsters used crypto bridge RenBridge to launder \$540 million, says report/ Including Russian and North Korean operations", *The Verge*, August 2022, accessed 6 October 2025, available at: www.theverge.com/2022/8/10/23299841/crypto-bridge-renbridge-used-launder-money-russia-north-korea-ransomware-report

44. See: [Arbitrum One Transaction Hash: 0xeafffae468... | Arbitrum One](#)

45. See: [Arbitrum One Transaction Hash: 0x62d61ee2b4... | Arbitrum One](#)

3.2.1.4. Liquidity pools

A liquidity pool, such as those used by AAVE, Balancer, or Curve.fi, is a smart contract-based mechanism that aggregates funds from multiple participants to facilitate on-chain financial transactions, most commonly token swaps and lending. Unlike traditional order books, the pool operates as a continuously available reservoir of assets.

Participants, known as liquidity providers, contribute token pairs or baskets (e.g. ETH/USDC) to the pool. In return, they receive liquidity provider (LP) tokens, which represent proportional ownership of the pool's assets and entitle holders to a share of transaction fees or yields generated by the pool.

Systemically, liquidity pools form the backbone of automated market makers (AMMs) and other DeFi protocols. They enable frictionless, permissionless exchange of digital assets while introducing new dynamics of risk, reward, and governance compared to centralised intermediaries.

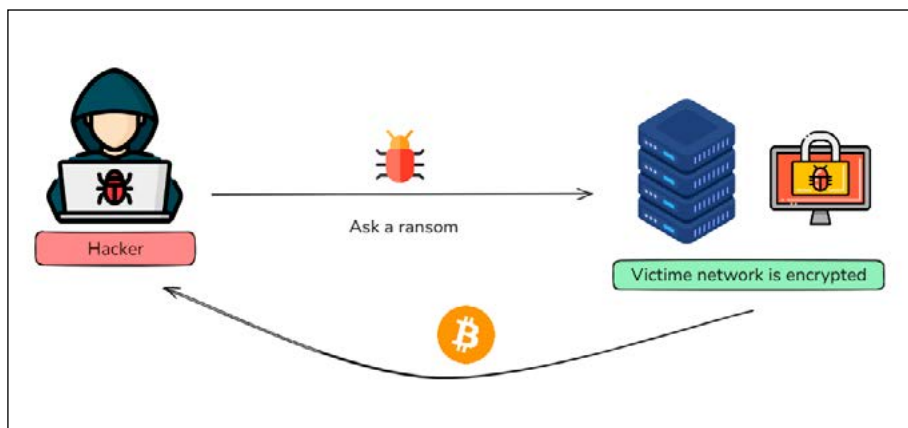
3.2.2. Defi as a new layer in money laundering schemes

3.2.2.1. A combination of various tools – the example of ransomware attacks

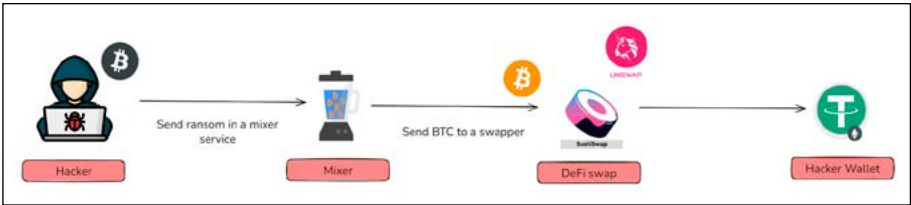
Ransomware attacks illustrate how DeFi is integrated into laundering chains. In a typical ransomware incident, attackers infiltrate a network, encrypt systems and ask for a ransom – often threatening to publish the stolen data if the payment is not made. Ransoms are generally required to be paid in crypto-assets, most commonly Bitcoin, as it is the best-known and easiest asset to obtain.

After receiving a ransom, perpetrators typically attempt to transfer the stolen funds through mechanisms designed to make tracing the flow of funds extremely difficult, if not impossible.

Although blockchains are public and make transaction flows visible, this visibility has encouraged criminals to develop more sophisticated laundering methods.



An example of a money laundering method involves a criminal using a mixer service to anonymise their funds before employing DeFi services to convert BTC into another crypto-asset, in this case USDT (stablecoin).



It was also observed that crypto-asset transactions in criminal circles were often initially linked to cyber disputes.

The rise in the value of some assets, notably Bitcoin, contributed to the widespread adoption of this payment system prior to the advent of decentralised finance. Ultimately, crypto-assets began to appear in financial cases, and are now present in all types of disputes.

3.3. DeFi as a target

The criminal exploitation of smart contracts’ vulnerabilities is one the greatest threats currently facing DeFi. Cyberattacks can be carried out by state-backed criminal groups with considerable resources and skills. With the rise of crimeware-as-a-service (CaaS), individuals with lower technical skills are also capable of launching high impact attacks.

3.3.1. Contract vulnerability

Smart contracts are most frequently coded in Solidity, a powerful and complex programming language that allows contracts to be tested in a virtual environment before being deployed on the blockchain.

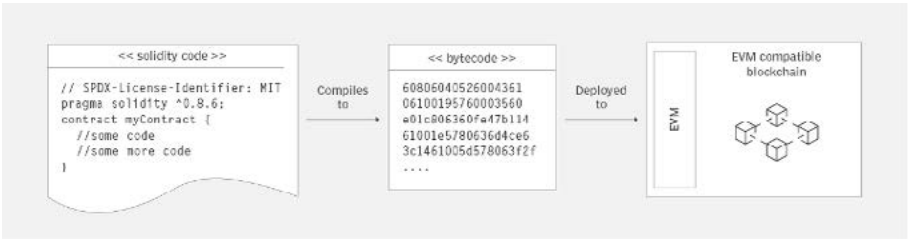
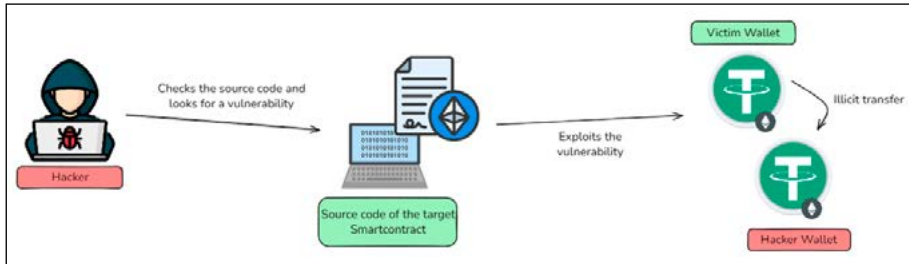


Illustration of the creation and testing of a smart contract⁴⁶

⁴⁶. Bob Reselman (2024), “Comment créer un smart contract sur Ethereum?”, LeMagIT, March 2024, [accessed on 17 November 2025], available at: www.lemagit.fr/conseil/Comment-creeer-un-smart-contract-sur-Ethereum

If a weakness is overlooked and discovered, hackers can hijack the function of a targeted smart contract to divert funds, as illustrated by the following case:



Platypus Finance is a DeFi protocol built on the Avalanche (AVAX) blockchain⁴⁷. It operates as an Automated Market Maker designed to swap stablecoins. In 2023, Platypus launched a new over-collateralised stablecoin, called USP. A simplified overview of its operation is as follows:

- ▶ Users can deposit stablecoins (e.g. USDT, USDC) as collateral to receive LP/USDC tokens;
- ▶ These LP tokens can either be staked to earn rewards or used as collateral to borrow USPs, up to a defined limit linked to the value of the collateral⁴⁸.

On 16 February 2023, Platypus experienced an attack that exploited a logical flaw in the collateral management and solvency checks of its USP stablecoin, resulting in a total loss of 9.05 million US dollars. The attack unfolded through the following sequence:

- ▶ The attacker borrowed 44 million US dollars in USDC through a flash loan;
- ▶ The USDC were used as collateral to get LP/USDC tokens;
- ▶ Using these LP/USDC tokens, the attacker borrowed USP tokens.

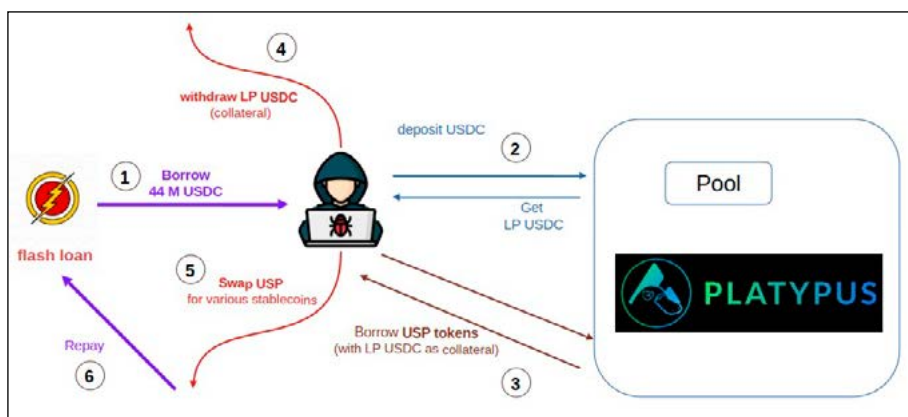
The attacker took advantage of an execution-order bug that failed to correctly verify the outstanding debt: this loophole allowed the attacker to withdraw the LP/USDC collateral without repaying the borrowed USP tokens. The borrowed USP was subsequently swapped for stablecoins, which allowed to repay the flash loan securing a profit.

The exploit partially drained the liquidity pools while also disrupting USP's peg. The Platypus team later patched the contracts and managed to recover a portion of the stolen funds.

This incident highlights the critical importance of rigorous business logic audits, testing smart contracts against flash loan scenarios, and implementing additional safeguards within protocol governance. More broadly, it underscores the necessity of thoroughly auditing and verifying smart contract code prior to deployment, as controlled testing environments can reveal vulnerabilities that might otherwise be exploited in production.

47. Shumba C. (2024), "Duo Behind \$9M Platypus Exploit Acquitted by Paris Court: Report", *CoinDesk*, March 2024, accessed 6 October 2025, available at: www.coindesk.com/policy/2023/12/04/duo-behind-9m-platypus-exploit-acquitted-by-paris-court-report

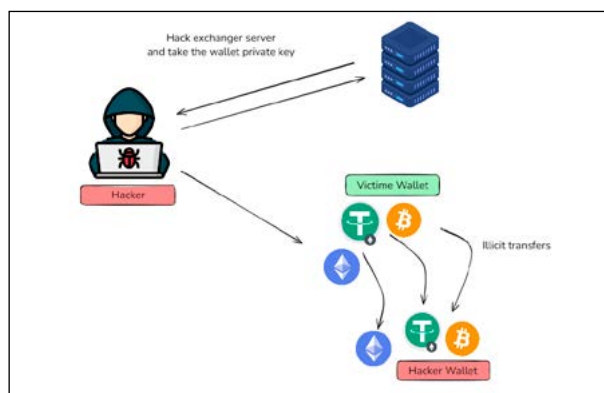
48. By doing so, users are accepting that if the collateral value dropped, their funds could be frozen or even liquidated.



3.3.2.Hacking

3.3.2.1. Infrastructure attacks

Hacking the infrastructure of a service or platform can also enable the theft of funds. When an exchange provides custody services, it holds the private keys of its customers' wallets. These keys are stored on servers administered by the exchange. If hackers gain access to the databases, and in particular the private keys, they can use them to empty the wallets of all customers.



3.3.2.2. Drainer

A drainer in crypto-assets is a malicious program – often a JavaScript script on a phishing site or a malicious smart contract – designed to automatically empty a wallet when the victim signs a trapped transaction. The attacker lures the victim to a fake page (airdrops, fake NFT mints, fake swaps), prompts them to connect their wallet, then asks them to sign a transaction or message that – disguised as a legitimate action – grants a broad permission (e.g. approve / setApprovalForAll or an EIP-712 / permit). Once the signature is obtained, the drainer can call a 'transferFrom' function or otherwise abuse the signed permission to move tokens instantly to his own addresses, sometimes splitting funds, swapping them, or routing them across chains to make tracing harder.

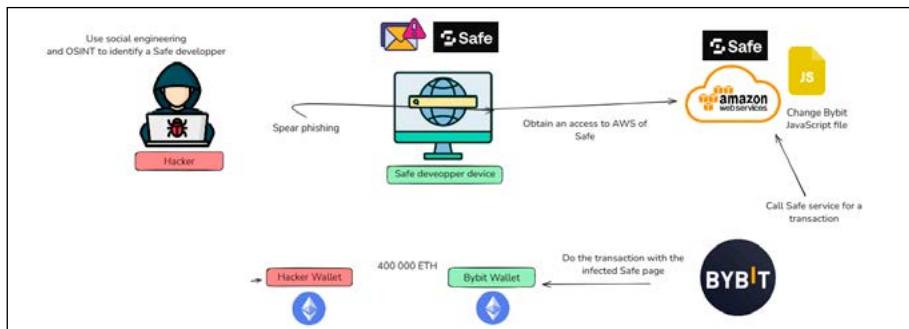
This phenomenon is rising alongside draining-as-a-service (DaaS)⁴⁹, where providers supply software and assistance to cybercriminals in exchange for a share of the proceeds (commonly around 20% to the coders/providers and 80% to the users⁵⁰).

3.3.2.3. Supply chain attacks

An even more sophisticated form of attacks involves targeting the supply chain rather than the platform itself. One of the most notable examples is the attack on the South Korean exchange Bybit in February 2025,⁵¹ which resulted in the theft of 400 000 ETH valued at around 1.5 billion US dollars at the time. This is the second largest theft of crypto-assets in recent years. The investigation determined that the platform was the victim of a highly sophisticated and meticulously planned operation.

Cold wallets – kept offline – are widely used by exchanges to store private keys more securely and limit the risk of hacking. To move funds from such wallets, Bybit required several signatories to validate the transaction through Safe's MultiSig system. The hackers compromised Safe's infrastructure through a malware that infected one of the developer's machines, most likely injected via a phishing campaign. Once they had gained access, they broke into the Amazon Web Service services used by Safe to manage its smart contracts and customers. Once inside, they identified the infrastructure related to Bybit and modified a JavaScript file in the backend of the MultiSig transaction authentication page.

The modification was designed to activate only for transactions above a certain threshold, allowing the attackers to remain undetected. On the user interface, the Chief Executive Officer of Bybit and his co-signatories saw the legitimate destination wallet address. However, in the backend, the code redirected the funds to wallets controlled by the hackers. In this way, the attackers successfully diverted 400 000 ETH without triggering alarms.



49. Blocksec (2024), "#5: Platypus Finance: Surviving Three Attacks with a Stroke of Luck", February 2024, accessed 13 October 2025, available at: <https://blocksec.com/blog/5-platypus-finance-surviving-three-attacks-with-a-stroke-of-luck>

50. Cyberscope (2024), "Drainer-as-a-Service (DaaS): Unmasking the Dark Web's Latest Threat", November 2024, accessed 13 October 2025, available at: <https://cyberscope.medium.com/drainer-as-a-service-daas-unmasking-the-dark-webs-latest-threat-e54ad69d12da>

51. Elliptic (2025), "The largest theft in history following the money trail from the Bybit Hack", *Elliptic Research*, February 2025, accessed 10 December 2025, available at: www.elliptic.co/blog/bybit-hack-largest-in-history

This highly sophisticated hacking attack has been attributed to the North Korean cybercriminal organisation Lazarus Group⁵².

This case highlights the growing appeal of crypto-assets, whose rising value attracts criminal groups with multiple skills, and in the case of Bybit, appears to have even been supported by governments.

3.3.2.4. Bridge hacks

In March 2022, the Ronin Network, a sidechain for the popular NFT game “Axie Infinity” developed by Sky Mavis, was hacked, resulting in the theft of approximately 173 600 ETH and 25.5 million USDC – a total value of around 625 million US dollars.

The attackers compromised the private keys of five out of nine validators, allowing them to authorise fraudulent withdrawals. The breach went undetected for six days until a user reported being unable to withdraw 5 000 ETH⁵³.

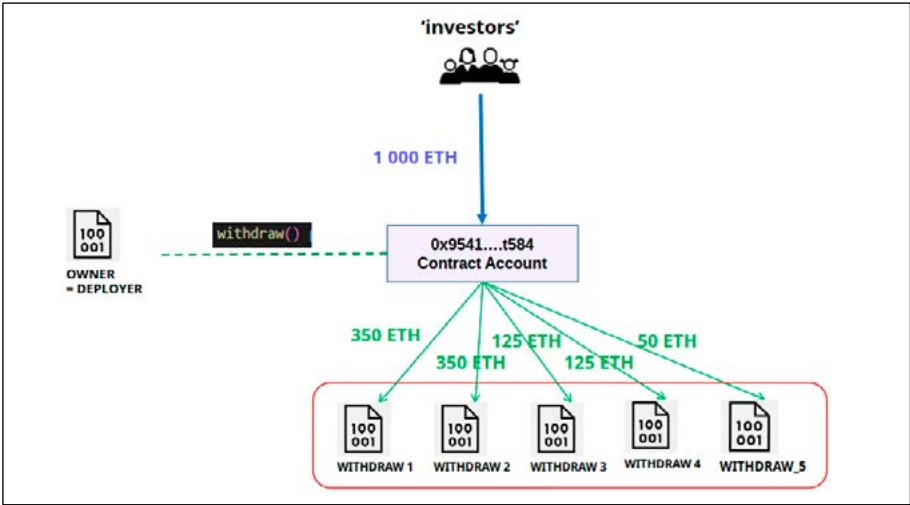
The FBI attributed the attack to the Lazarus Group.

3.4. Defi as a perpetrator

3.4.1. Malicious use of contracts – rug pull scams

In this scheme, the project’s team either manipulates the assets it collects or inserts malicious functions into the project’s code to perform an exit scam and defraud users.

The project is typically promoted through social media or messaging apps, sometimes amplified by influencers. Victims are persuaded to invest and purchase tokens with promises of high returns. Once the scammer decides that enough funds have been raised, all assets are withdrawn, causing the token price to collapse.



52. See: https://en.wikipedia.org/wiki/Lazarus_Group
53. Behnke R. (2022), “Explained: The Ronin Hack – March 2022”, Halborn, March 2023, accessed 6 October 2025, available at: www.halborn.com/blog/post/explained-the-ronin-hack-march-2022?utm_source=chatgpt.com

To siphon funds in this example, the scammer triggers a ‘withdraw’ function embedded in the smart contract code. This function automatically transfers the collected funds to five different non-custodial addresses under the scammers or accomplices’ control, according to a predefined allocation (35%, 35%, 12.5%, 12.5%, and 5%).

Extract of the decompiled version of a smart contract, with the function name in blue, the receiving address in yellow and the distribution key in red (Source: Etherscan.io⁵⁴)

Wash trading consists of artificially inflating trading volumes by repeatedly buying and selling the same asset, creating a false impression of market demand.

54. See: [Online EVM Bytecode Decompiler](#), accessed 9 September 2025

FTX, a cryptocurrency exchange founded by Sam Bankman-Fried, collapsed in November 2022 after it was revealed that customer funds were improperly diverted to Alameda Research, a trading firm also controlled by Bankman-Fried. The misuse of client deposits, combined with poor risk management and conflicts of interest, led to billions of dollars in losses for investors. The scandal triggered widespread regulatory scrutiny and criminal investigations in the United States and internationally and is considered one of the largest crypto-related frauds to date.

3.5. Defi as an intermediary

3.5.1. Crypto-assets-based investment fraud and romance bait

Investment fraud associated with crypto-assets is one of the fastest growing crime segments. Using increasingly sophisticated tactics, perpetrators lure victims into depositing money into fraudulent financial “investments” involving crypto-assets. Victims may even be encouraged to open accounts with legitimate exchanges. Another common method involves fake advisers persuading victims to install remote access software (such as AnyDesk or TeamViewer) under false pretences (e.g. monitoring purposes), allowing the scammers to gain access to their accounts.

Romance bait, also known as pig butchering, is a related type of romance scam. Perpetrators gradually build an online relationship with a victim, using emotional manipulation before convincing them to invest in a business or scheme⁵⁵.

Both investment fraud and romance bait illustrate how crime adapts to technology – particularly to DeFi⁵⁶. An increasing number of cases involve the use of DeFi applications, which offer clear advantages to scammers, notably by giving them direct control over the victims’ funds.

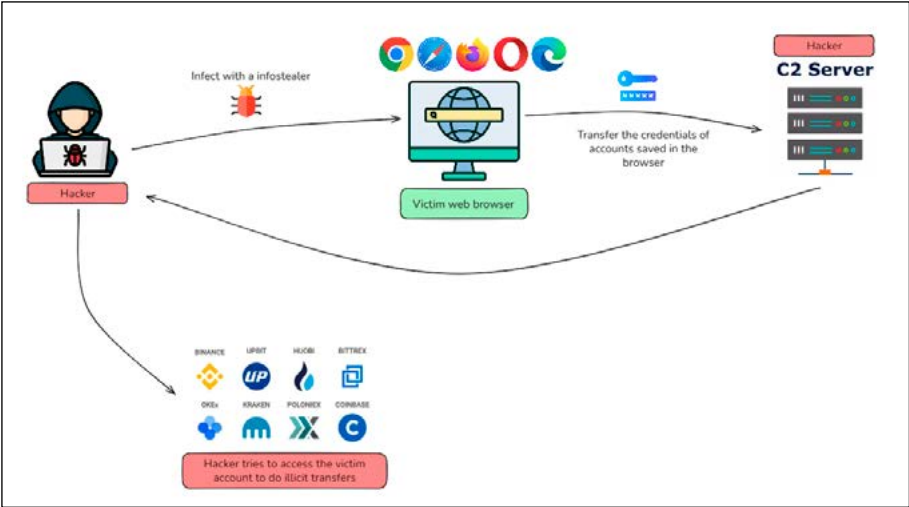
3.5.2. Phishing / stealing private keys

Some attacks target the data of wallet holders, particularly their private keys. Once obtained, these allow criminals to carry out illegal transactions.

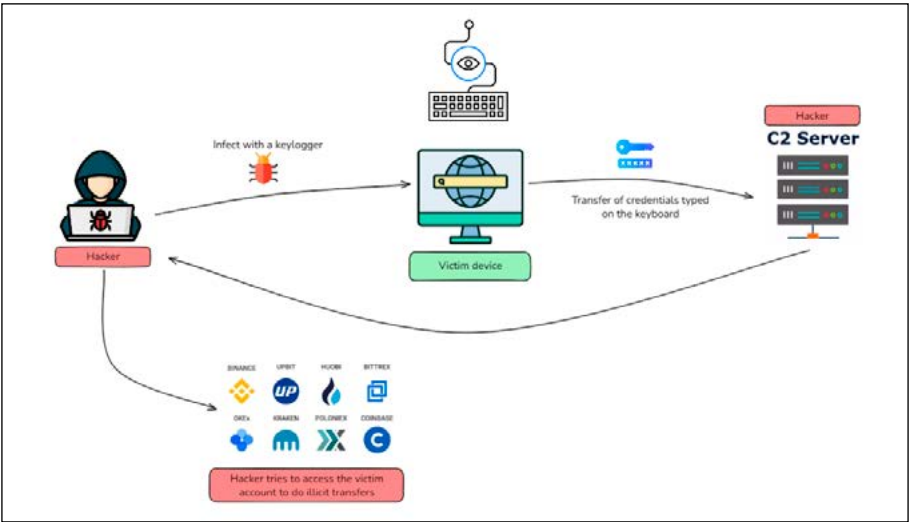
One widespread method involves malware known as “stealers” by criminals. These are designed to steal all logins/passwords stored in web browsers (Firefox, Chrome, and other). Among these stored credentials are access details for crypto-asset exchanges such as Binance, Crypto.com, and other. While two-factor authentication mechanisms provide some protection, these attacks can be combined with “login cookie capture”, enabling them to bypass security measures.

55. Gallagher S. (2024), “Cryptocurrency scams metastasize into new forms”, Global Network on extremism and technology, October 2024, accessed 6 October 2025, available at: <https://news.sophos.com/en-us/2024/02/02/cryptocurrency-scams-metastasize-into-new-forms/>

56. Roul A. (2024), “The Rise of Monero: ISKP’s Preferred Cryptocurrency for Terror Financing”, Global Network on extremism and technology, October 2024, accessed 6 October 2025, available at: <https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/>

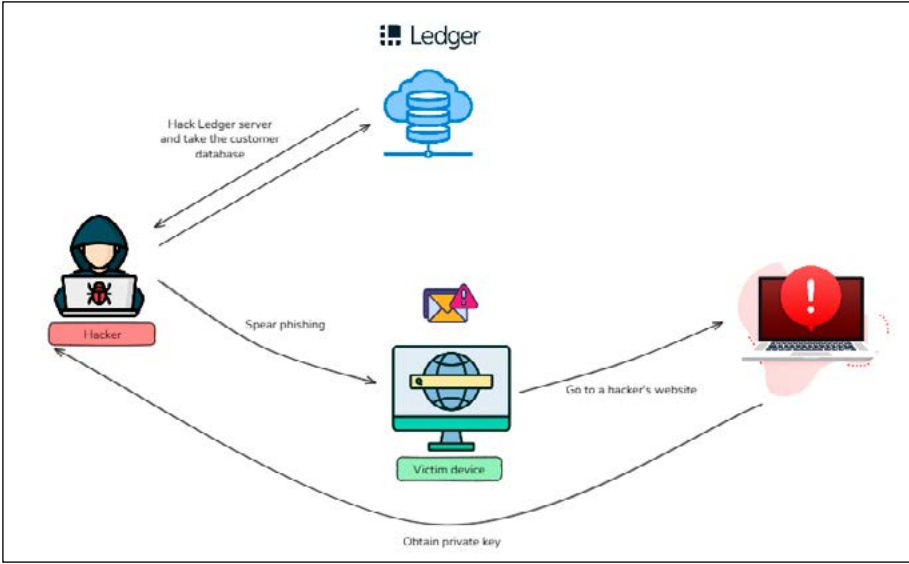


A variation of this technique involves the use of another type of malware called “keyloggers”. This involves capturing keystrokes from an infected machine in order to obtain credentials and then attempt to log in to exchanges to initiate fraudulent transfers.



Importantly, attempts to obtain private keys do not only concern holders of online wallets. Users of cold wallet have also been targeted. One example involved Ledger, a well-known hardware wallet provider.

Following a hack in which customer databases were stolen, attackers launched spear-phishing campaigns against Ledger clients. Victims received personalised emails prompting them to connect to fraudulent websites where they were tricked into entering their recovery seed phrase and PIN code. With this information, attackers were able to regenerate accounts on new devices and perform unauthorised transfers.



Phishing campaigns can also target more traditional exchanges and aim to obtain login details and passwords. However, the Ledger case is particularly noteworthy because cold wallets are considered more secure, demonstrating that even the more trusted security solutions can be compromised through sophisticated attacks.

This overview of risks highlights the growing use of decentralised finance and crypto-assets by criminal groups. In response, intelligence agencies and law enforcement agencies in various countries have had to adapt and seek specific investigative methods relating to these assets.

4. Tools and resources for investigations

A blockchain is like a public ledger in which all transactions are recorded and stored. For each transaction, data such as the amount, date (timestamp), sender, and recipient are accessible. This transparency is a major asset for investigators.

Senders and recipients can be identified by their respective public addresses, which consists of a long alphanumeric character string. This is referred to as pseudonymity, as the true identity of the individuals behind these addresses is not directly apparent.

The main challenge of an investigation is to link these addresses and transactions to a natural person or entity. This process, known as attribution, involves connecting a transaction or address to a real-world individual. When crypto flows involve a CASP, identification is made easier since CASPs are required to collect and store its customers' identification details (KYC) and can provide them upon request of law enforcement or judicial authorities. Identification can also sometimes be inferred from open source intelligence (OSINT).

Crypto investigations can be divided into three steps: detection, tracing and identification.

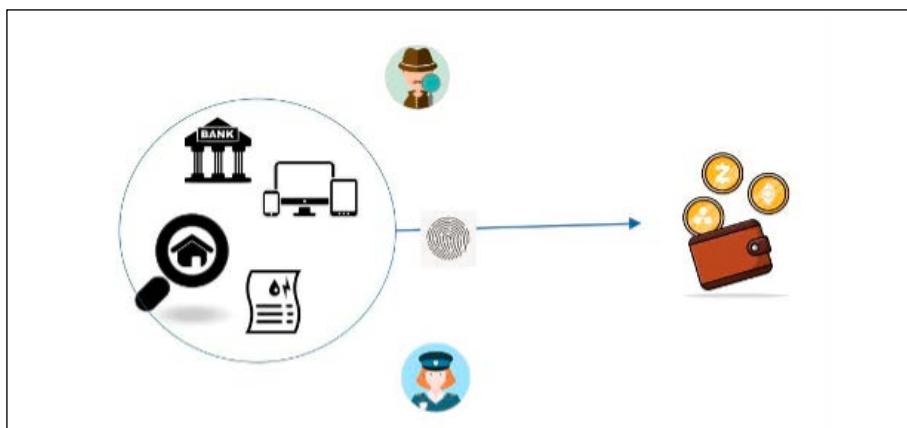
4.1. Crypto analysis – step by step

4.1.1. Detecting

The first step is to find evidence suggesting the presence and use of crypto-assets.

In financial investigations led by financial intelligence units (FIUs), the aim will be to detect crypto-fiat conversion points (known as cash-in/cash-out transactions) in bank statements or other financial/non-financial documents (e.g. invoices, wire transfer details, evidence of hardware purchases such as storage keys, foreign account declaration forms, associated accounts, and other).

In the context of a police investigation, traces may be obtained during house searches and forensic analyses, revealing the presence of dedicated software, passwords, seed phrases, purchase invoices, and other indicators of crypto usage.



4.1.2. Tracing

The next step consists in applying the traditional “follow the money” method, tracking crypto transactions using specific tools (blockchain explorers) and techniques.

A main objective is to trace funds to an exchange platform, which can be requested to provide the identity of the individual behind the transactions. Conversely, attempts can be made to trace the origin of the funds, again with a view to identifying associated addresses. This process also allows investigators to analyse the composition and use of criminal's portfolio.

4.1.3. Identifying

Portfolio identification involves identifying custodial and self-hosted addresses likely linked to an individual or group, forming their wallet. This work enables to:

- ▶ establish the financial profile of the target based on the volume and usage of the wallet (e.g. investor, money launderer, victim, mule, and other);
- ▶ detect addresses with positive balances ('unspent'), which may contain proceeds of crimes (e.g. fraud or ransomware).

User identification aims to link wallets to individuals with high certainty. That's where centralised and regulated platforms play an essential role, serving as the main entrance and exit points for crypto while acting as gatekeepers.

4.2. Specifics of DeFi-related investigations and analysis

The use of DeFi platforms and applications significantly complicate investigations. On one hand, the very nature of the sector makes it impossible to automatically identify users, who have complete autonomy in managing their own transactions and controlling their portfolios. There is no identification (KYC) required to use the decentralised applications. Unlike centralised platforms, there is no entity that can be subjected to requests from law enforcement agencies.

On the other hand, the use of DeFi platforms and applications introduces additional challenges for investigation:

- ▶ The crypto-assets trail can be made much more complex, as users may move different assets across different blockchains, and sometimes employ anonymity-enhancing solutions, such as mixers;
- ▶ The ability to switch rapidly between assets is multiplied;
- ▶ Transactions can be executed within extremely short timeframes;
- ▶ DeFi-related cases require additional technical expertise from investigators.

Despite these obstacles, the investigative process is far from impossible, albeit more laborious. With meticulous analytical work and equipped with the right tools and resources, it remains possible to detect sophisticated fraud schemes, identify perpetrators and seize illicit assets.

4.3. Smart contracts' analysis

Some cases demand the ability to read and interpret smart contracts in order to understand their nature, environment, functions and potential for fraudulent use.

One of the first steps is to convert the code into a usable format. Smart contracts are typically written in Solidity and then compiled into bytecode, a format that is difficult to interpret for non-experts. The decompilation process – i.e. translating the code back into a more readable form – is often integrated into blockchain explorers such as Etherscan.

Once this conversion has been completed, investigators can extract a range of useful information:

a) *Basic elements* such as:

- ▶ The address itself, known as the contract address (CA);
- ▶ The deployment address, which is an externally owned account (EOA) which initiates the contract launch;
- ▶ The public nature of the code and its verification status.

ETH addresses and transactions

A smart contract can be deployed through a blockchain transaction initiated either by another smart contract or by an externally owned account, also called the deployment address.

- ▶ *Externally owned accounts* are standard user addresses, generated from a private key. They serve as entry point for interacting with the Ethereum blockchain.
- ▶ *Contract accounts* or contract addresses, store and execute code only when triggered by a transaction from an EOA or another contract. A contract cannot execute on its own – there must always be an initial EOA-initiated transaction somewhere in the chain.

There are three main types of transactions:

- ▶ *EOA-to-EOA transactions*, which represent standard transfers, with one EOA sending ETH to another (similar to a Bitcoin transaction).
- ▶ *EOA-to-CA transactions*, where an EOA interacts with a contract by sending a transaction to it.
- ▶ *EOA-to-CA deployment transactions*, where an EOA creates a new smart contract (no ETH is transferred except for the gas fee).

b) The *analysis of the code* itself helps clarifying:

- ▶ The different functions it contains (transfer, mint, burn, withdraw, admin, and other);
- ▶ The different roles (owner, admin, MultiSig, and other) as well as the addresses to which they are assigned, which makes it possible to establish a relational graph.
- ▶ Among these roles, the most critical are *owner* and *admin*:
 - The *owner* is typically the account (EOA or MultiSig) that deployed the contract. Holding the highest level of control, the owner can transfer ownership and assign or revoke admin rights.
 - *Admins* are addresses or accounts that have been granted specific permissions, such as pausing deposits or withdrawals, or adjusting protocol parameters (e.g. interest rates in a lending protocol).

c) The *analysis of transactions* indicates the type, frequency, volume of operations, as well as the assets involved:

- ▶ Event logs (transfers, deposits, swaps, and other);
- ▶ Internal transactions;
- ▶ Flow tracking (tokens in and out, swaps, and other).

d) *Behavioural analysis*:

- ▶ Fraud indicators (copycat, specific functions such as withdraw or call);
- ▶ Usage patterns (flash loan, oracle manipulation, and other).

e) *Environment analysis* can be useful to detect:

- ▶ Related contracts;
- ▶ Clusters of addresses interacting with the contracts;
- ▶ Adverse coverage or other useful off-chain intelligence (GitHub developer, Telegram groups, scam websites, and other).

Decrypting a smart contract: the PABC case⁵⁷

The contract address 0x5DF340b5D1618c543aC81837dA1C2d2B17b3B5d8 corresponds to a token launched in October 2021 under the name *Party Ape Billionaire Club (PABC)*⁵⁸. This project was one of many created during the NFT boom at the end of 2021.

57. This case is used for pedagogical reasons, this does not mean it is necessarily a scam.

58. See: [Party Ape Billionaire Club: PABC Token | Address: 0x5df340b5...b17b3b5d8 | Etherscan](#)

Below are some key findings from the analysis of this address:

1. Team addresses

Examination of the smart contract code identifies four TEAM addresses, each associated with an equal share of 25%. These addresses are presumably controlled by the project's developers or initiators.

```
30     Counters.Counter private _tokenIds;  
31     uint256[] private _teamShares = [25, 25, 25, 25];  
32     address[] private _team = [  
33         0x8dD47E819c53138aA18F8651D797e7969f34d1F1,  
34         0xF536390c3A0bAFF71289975e45e1f647fc8C7304,  
35         0xFD6Ed83d8e47B1C808efE984cEF965B2CB3393De,  
36         0x03bb7A8226301C1c0e82BFf029989E22a76F597
```

Source: Etherscan.io

2. Funding and related addresses

- ▶ The contract was deployed on 14 August 2021⁵⁹ by the EOA 0xfd6ed83d8e47b-1c808efe984cef965b2cb3393de, designated as the initial owner and also referred to as the PABC Deployer. This address is one of the four TEAM addresses.
- ▶ The same address created another token (*Cyborg Billionaire Dog*) three days later.
- ▶ Prior to deploying PABC, the PABC Deployer was funded by thebossofbali.eth (0x3858548E1D069730C3871937039D86F0DCF007a3).
- ▶ thebossofbali.eth itself received funds from several CASPs (Binance, Kraken, and KuCoin⁶⁰).
- ▶ thebossofbali.eth has also held an account with the NFT trading platform OpenSea since September 2021 (see screenshot, p. 50).

Given these links, the person controlling the thebossofbali.eth address is very likely connected to the project. Requests could be made to the relevant CASPs to obtain transaction histories and KYC details for the custodial wallets funding this address.

3. Tracing the proceeds

Addresses	Token	TokenID	Balance	Value In USD	Total Value In USD
PABC [contract]	ETH	-	20.5	\$72,851.9	\$72,851.9
0x1930200c3a0ba171289975e45e1f647fc8c7304	ETH	-	-20.5	\$72,851.9	-\$72,851.9

From	To	Value	Gas Used	Gas Price	Transaction Hash
0x1930200c3a0ba171289975e45e1f647fc8c7304	0xfd6ed83d8e47b1c808efe984cef965b2cb3393de	20.5 ETH	21,000	35 Gwei	0x1930200c3a0ba171289975e45e1f647fc8c7304

Example of one of these transactions (Source: Blocksec/Phalcon⁶¹)

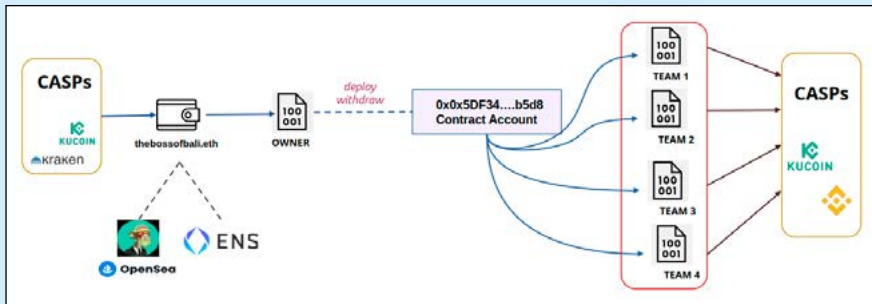
59. See: [Ethereum Transaction Hash: 0x513011938a... | Etherscan](#)

60. See: [thebossofbali.eth | Address: 0x3858548e...0dcf007a3 | Etherscan](#)

61. See: [0x4fcdaf8154a7fa4656 | Phalcon Explorer](#)

The analysis of the recipient addresses reveals further links with CASPs, including KuCoin and Binance. Requests for information from these providers could assist in identifying the individuals who ultimately benefitted from the proceeds of the project.

This case could be summarised as follows:



These links and transactional flows can be visualised using open source blockchain analysis tools (see p. 46).

4.4. Some useful tools and resources

Nota Bene: Chapter 8 contains a list of some useful and relevant links. The tools and resources mentioned in this list, or below, are provided for illustrative purposes only. Their inclusion does not constitute a recommendation. It is up to each investigative service, based on its level of expertise and specific needs, to choose the resources it deems most appropriate.

A wide range of solutions exist to aggregate, present and enrich the vast amount of public data available on blockchains. These resources can be divided into three categories:

- ▶ *Blockchain explorers* (block explorers) provide a detailed view of one or more blockchains through their transactions, blocks and addresses. By enabling the tracing of crypto-asset flows, they are a fundamental tool for any investigator. Some are dedicated to a specific blockchain (such as Etherscan, Mempool or Wallet Explorer), while others, known as multichain explorers, cover several blockchains (Blockchair, DeBank, Blockchain.com, and other).
- ▶ *On-chain data providers* offer a more structured view of blockchain data, which can sometimes be queried via an application programming interface (API).
- ▶ Finally, some platforms offer *more sophisticated analyses* of blockchains, markets or specialised assets (tokenomics).

By making on-chain data accessible to anyone and enriching its content, these solutions provide resources that facilitate crypto research and investigations at a lower cost.

Alongside these open source tools, a number of private market specialised software operate through paid licences. These products are aimed at financial institutions' compliance units (banks and CASPs), regulators, law enforcement agencies, and

judicial authorities. Chainalysis, Caudena (formerly Clain), Crystal Intelligence, Elliptic and TRM Labs are among the best-known players in the field.

Although paid tools historically offered far more comprehensive enrichment than free alternatives, this gap has gradually narrowed. Today it is possible to conduct even complex investigations using open source or freely available tools, as shown by many independent investigators operating online. Moreover, several private providers now offer free access to part of their features.

The following sections provide an overview of available tools, outlining their main advantages and limitations.

4.4.1. Blockchain analytics software

The main advantages of commercial solutions include:

- ▶ Strong attribution capabilities, grouping addresses into multiple categories such as exchange platforms, services, DeFi protocols, dark markets, illicit activities (terrorist financing, child sexual abuse material), sanctioned addresses or self-hosted wallets (such as Metamask);
- ▶ Extensive data enrichment through cross-referencing with open sources and technical data (including geolocation via Internet Protocol (IP) addresses);
- ▶ Advanced heuristics enabling address clustering and therefore wallet identification;
- ▶ Multi-chain coverage, enabling simultaneous work across multiple blockchains⁶²;
- ▶ Graphical visualisation of flows and relational graphs.

In addition, these companies offer specific solutions to facilitate the work of investigators through investigation reports on a specific theme or portfolio, the implementation of real-time alerts, demixing capabilities (i.e. the ability to trace transactions through mixers whose purpose is precisely to prevent the traceability of funds), the possibility to share data with fellow analysts, between users, and other.

- ▶ Despite their sophistication, these tools are not without limitations, although marginal, whereas attribution errors remain possible. For example, the address of a CASP relying on another CASP for part of its services may be wrongly tagged as belonging to the latter. Similarly, a “nested service” will be incorrectly linked to the service that hosts it.
- ▶ Inter-service compatibility should also be mentioned: if a service relies on tool A to carry out its investigation, it is very likely that it will use and share the resulting graph (in native format). If the recipient, whether a judicial authority or another investigative service, wishes to use these elements to enrich or verify them, it would also need a licence.
- ▶ The probative value of the data provided by these companies should also be questioned. It is likely that an analysis produced by such software cannot stand alone in court. Investigators must be able to explain and reproduce their own tracing to ensure judicial admissibility.

62. Provided that these blockchains are supported by the tool and included in the licence.

- ▶ Confidentiality and sovereignty concerns arise especially for sensitive cases, when relying on external service providers.
- ▶ Finally, investing in external software can pose a risk of dependency, not to mention the uncertainty that would surround the sudden bankruptcy of the company behind it.

Nevertheless, thanks to continuous improvements, these tools remain valuable allies in complex investigations, as evidenced by the numerous results obtained with their support by many government agencies (and which are the subject of skilful communication). However, it is important to avoid the pitfall of relying solely on these solutions, in particular by developing autonomous investigation capabilities based on freely available data and tools.

4.4.2. Blockchain explorers and free access tools

Given their accessibility, number and variety, free tools are of undeniable interest to LEAs and FIUs. They can be used not only in operational investigations and forensic analysis, but also as training material. They are excellent and indispensable educational tools, enabling users to understand and master the subject matter, track transactions across multiple blockchains, get to the heart of smart contracts and other.

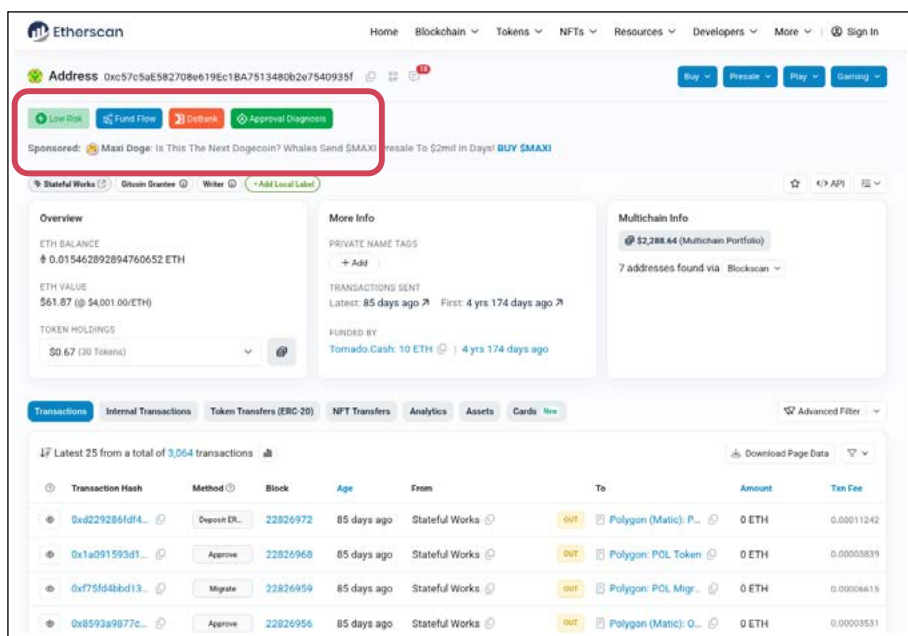
The development of new free tools and resources in recent years has made it much easier to conduct thorough investigations without commercial solutions.

It should be noted that the confidentiality rules quoted above for private software also apply to these solutions. Open source crypto research must comply with the rules and precautions applicable to OSINT investigations.

Each blockchain has its own specific features, and generally at least one – sometimes several – public block explorers are available for it. Many of these explorers replicate the model of Etherscan, the leading explorer for the Ethereum blockchain.

The screenshot displays the OP Mainnet blockchain explorer interface. At the top, there's a navigation bar with links for Home, Blockchain, Tokens, NFTs, Resources, Developers, and More, along with a Sign In button. The main content area shows the details for an address: 0xc57c5a58270e619e018a7913480b2e754093bf. It includes buttons for 'View', 'Copy', and 'Generate'. Below this, there are tabs for 'Overview', 'More Info', and 'Multichain Info'. The 'Overview' tab is active, showing the ETH balance as 0.0224969585425650156 ETH, the ETH value as \$939.34, and token holdings. The 'More Info' tab shows private name tags, transactions sent, and funded by information. The 'Multichain Info' tab shows a balance of \$2,288.64 and 7 addresses found via Blockscan. At the bottom, there's a 'Transactions' section with a table of recent transactions. The table has columns for Transaction Hash, Method, Block, Age, From, To, and Amount. It shows three transactions, all of type 'Transfer', with their respective hashes, block numbers, ages, and amounts in ETH.

Transaction Hash	Method	Block	Age	From	To	Amount
0x72b171ae3d...	Transfer	9666088	871 days ago	0x72b171ae3d...	0xc57c5a58...a754093bf	0.05 ETH
0x4995b17d19...	Transfer	73384717	958 days ago	0x71b94278...8d68b0d4c	0xc57c5a58...a754093bf	0.005 ETH
0x948dc0e795...	Transfer	69170273	979 days ago	0x948dc0e795...	0xc57c5a58...a754093bf	0.0224969585425650156 ETH



Source: Compared screenshots of Etherscan⁶³ and Optimism⁶⁴ for a randomly selected address (0xc57c5aE582708e619Ec1BA7513480b2e7540935f)

Among notable initiatives, the cybersecurity company BlockSec has developed several tools useful for blockchain investigations:

- ▶ MetaSleuth, a tracing platform equipped with a graphical visualisation interface;
- ▶ MetaSuites, a browser extension that enhances data from explorers such as Etherscan by attributing addresses, offering user-friendly graphical visualisations, detailing smart contract functions and enabling direct portfolio analysis via Debank (as illustrated in the red rectangle above).

4.4.3. Smart contracts analysis

Smart contract code analysis involves a combination of manual review, automated scanning, and runtime testing to identify vulnerabilities and ensure protocol integrity.

At the *manual level*, auditors examine the source code to understand business logic, review function visibilities, permissions, and modifiers, and detect common pitfalls such as unsafe use of 'tx.origin', unprotected owner functions, or gas-intensive loops.

Automated static analysis tools – such as Slither, Mythril, Securify, or Oyente – help detect known vulnerabilities directly in the source code or bytecode. This is complemented by *dynamic analysis*, where contracts are deployed in local or test environments (Ganache, Hardhat, Foundry). Running *unit tests* and applying fuzzing techniques with tools such as Echidna may expose unexpected behaviours, including re-entrancy or arithmetic issues.

63. See: [Stateful Works | Address: 0xc57c5aE5...e7540935f | Etherscan](#)

64. See: [Address: 0xc57c5ae5...e7540935f | OP Mainnet Etherscan](#)

When source code is unavailable, auditors rely on *reverse engineering* of EVM byte-code using disassemblers like ethersvm, Ghidra, or IDA to identify high-risk Operation Codes (Opcodes) such as ‘delegateCall’ or ‘selfDestruct’.

For high-assurance projects, *formal verification frameworks* (KEVM, Certora) mathematically prove that specific security properties hold, reducing the risk of critical flaws.

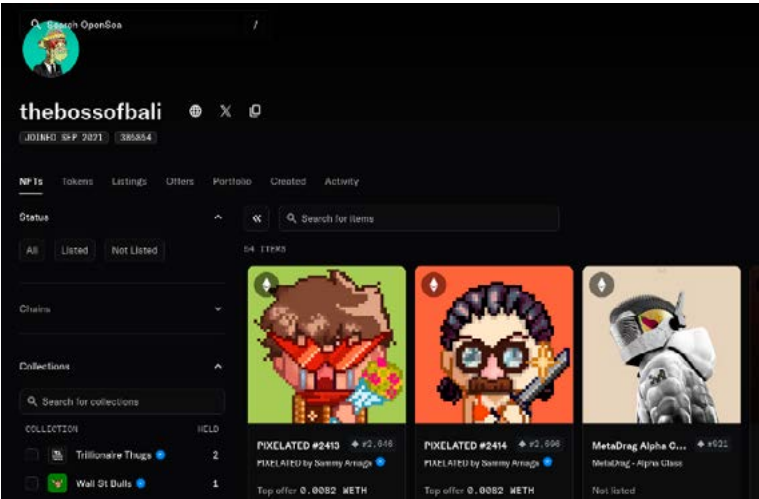
Finally, *post-deployment monitoring* is crucial. Services like Tenderly or Forta provide real-time tracing and alerts for suspicious patterns, enabling early detection of vulnerabilities or active attacks.

4.4.4. Other OSINT tools for crypto investigations

4.4.4.1. NFT platforms

Platforms such as OpenSea, Rarible, and SuperRare are dedicated to the NFT market. They contain the history of transactions involving NFTs and can be used to:

- ▶ establish the ‘assets’ and activity of a specific address;
- ▶ corroborate suspicions of theft (e.g. when the transfer of an NFT is not accompanied by the corresponding payment);
- ▶ identify NFTs used as profile pictures on a social network, through searches based on the specific characteristics of the image.



Source: OpenSea account for address 0x3858548e....f007a3 (thebossofbali)⁶⁵

4.4.4.2. Github

GitHub is a collaborative platform for software development and code sharing. It provides access to a vast array of information shared by developers and communities.

⁶⁵. See: [thebossofbali - Profile | OpenSea](#)

4.4.4.3. Scam databases

Collaborative initiatives – whether independent or linked to the blockchain industry – provide extensive information on scams, hacks, and exploits, often with technical breakdowns of the issues involved. Communities on platforms such as Reddit's *r/ethereum*⁶⁶ and Twitter (X) also circulate real-time scam alerts and red flags, serving as valuable open source intelligence for investigators⁶⁷.

4.4.4.4. Telegram groups

In May 2025, Telegram shut down two major channels⁶⁸. One of them, the Xinbi Guarantee marketplace, had laundered over 8.4 billion US dollars in USDT since 2022. Its services included money laundering, the sale of stolen data, and the provision of counterfeit documents – demonstrating how Telegram-based stablecoin networks have grown into major vectors for illicit finance, surpassing the scale of traditional darknet markets.

Some services operate through Telegram bots, which facilitate client interactions without identity checks. Certain centralised platforms, such as Kyrrex, even allow limited operations via Telegram with no KYC requirements. Reports also indicate that encrypted messaging apps are increasingly being used to provide DeFi-style laundering services, underscoring the convergence between messaging platforms and decentralised finance in enabling illicit activity.

A recent TRM Labs report⁶⁹ highlighted a US law enforcement operation that dismantled a laundering network moving more than 24 million US dollars through darknet markets and peer-to-peer platforms. Investigators, by covertly operating part of the service, traced flows through intermediary wallets and linked them to Telegram/WhatsApp communications, ultimately unmasking the operator.

4.4.4.5. Social media

The crypto sector is heavily promoted across major social media platforms⁷⁰. Large players maintain well-established channels with millions of followers, while smaller DeFi protocols use the same outlets to attract new users through promises of high-yield products, token listings, or reward campaigns.

In parallel, influencers – social media personalities specialising in crypto promotion – often amplify risky or fraudulent projects. Additional investigative leads can also come from domain registration data (WHOIS), which helps attribute suspicious websites used in scams and rug pulls.

66. See: [Ethereum](#)

67. See a proposed list of high-risk dApps: <https://dappradar.com/rankings/high-risk>

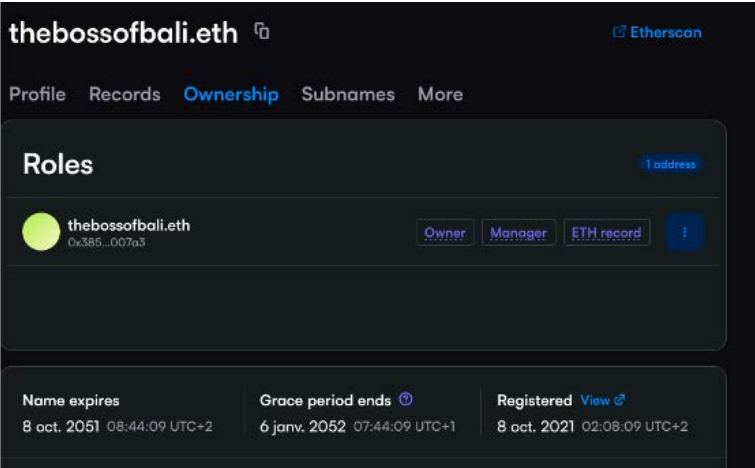
68. Elliptic (2025), "Xinbi: The \$8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers", *Elliptic Research*, May 2025, accessed 6 October 2025, available at: www.elliptic.co/blog/xinbi-guarantee?utm_source

69. TRM Labs (2025), "US Law Enforcement Dismantles \$24M Dark Web Crypto Laundering Network", *TRM Blog. Insights*, April 2025, accessed 6 October 2025, available at: www.trmlabs.com/resources/blog/us-law-enforcement-dismantles-24m-dark-web-crypto-laundering-network

70. Mihajlović M. (2023), "A Guide to Crypto Twitter", *Shrimpy Academy*, May 2023, accessed 6 October 2025, available at: <https://web.archive.org/web/20250327071713/https://academy.shrimpy.io/post/a-guide-to-crypto-twitter>

4.4.4.6. Ethereum Name Service (ENS)

ENS is a decentralised, open source protocol for renaming addresses on the Ethereum blockchain, facilitating transactions by reducing the risk of errors associated with address transcription.

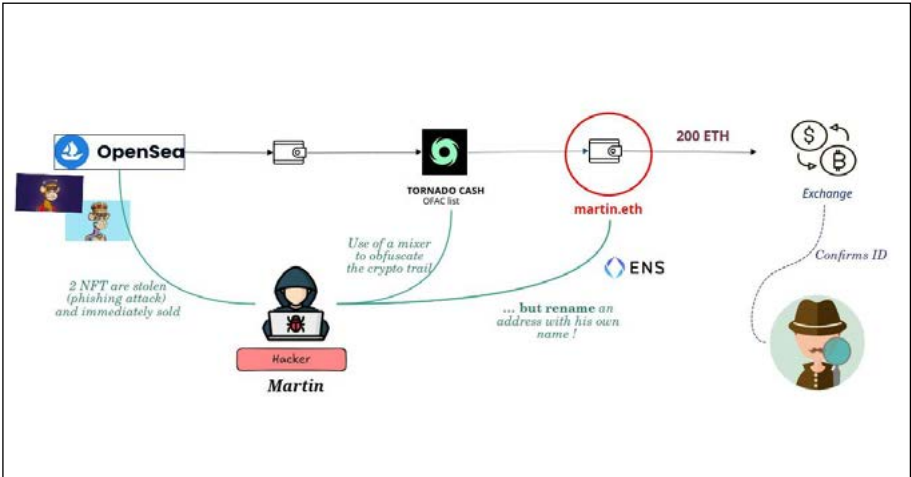


Source: app.ens.domains

Adress **0xafbf632.....ac79810** was renamed thebossofbali.eth on 8 Octobre 2021.

ENS’ features also offer the opportunity to facilitate user identification by:

- ▶ cross-referencing ENS names with other platforms where this name could be used social media, NFT sales platforms, and other;
- ▶ tracing the origin of funds associated with the ENS-registered address.



In the above case example, OSINT data helped identify a hacker who had stolen NFTs from their owner. After immediately selling them on OpenSea, he transferred the funds through several addresses and used Tornado Cash to obfuscate the origin of the crypto-assets deposited with a CASP to acquire real estate. Investigations initially focused on:

- ▶ the hacker's activity on the OpenSea platform, allowing the identification of other NFT thefts;
- ▶ reconciliation of incoming and outgoing funds from Tornado Cash (demixing).

The breakthrough came from an operational mistake. The hacker renamed one of his self-hosted wallets' addresses with his real first name via ENS. This attribution error enabled investigators to link him conclusively to the theft.

5. Limitations and challenges

5.1. A strengthened tough perfectible framework

With the exception of a few decentralised platforms subject to recent national and European regulatory developments (e.g. Tether and Circle), DeFi remains largely beyond the reach of investigative services and judicial authorities, presenting a major challenge for regulators. However, the responsibilities within many so-called decentralised protocols are often less dispersed than their names imply – a phenomenon sometimes called as “decentralisation theatre” – which opens potential avenues for regulation.

In theory, DeFi cannot be regulated in the same way as the traditional financial system:

- ▶ Users are not required to disclose their true identities – a simple wallet address is usually sufficient to interact with a DeFi application.
- ▶ Authorities cannot easily determine the volume of activity associated with a given portfolio, as there are no formal intermediaries to which information requests can be addressed.

From this perspective, DeFi can serve as both a safe haven and a potential hotspot for cybercriminal activity, operating largely beyond the reach of authorities. Nonetheless, the intersection points between DeFi and the regulated financial system may provide valuable entry points for regulatory action.

5.1.1. The limited role of CASPs as gatekeepers

Under the recently implemented EU regulation (i.e. MiCA), CASPs are expected to play a key role in facilitating wallet-holder identification and detecting suspicious activity. Jurisdictional arbitrage, however, limits this ambition:

- ▶ While the majority of large exchanges have decided to comply with the new rules, with the aim of keeping or developing their customer base (mainly in Europe), some, including major ones, continue to operate from jurisdictions considered to be non-cooperative, or having lower requirements and supervision powers. These jurisdictions appear as cybercriminal hotspots and safe havens from which it is difficult, if not impossible, to obtain information.
- ▶ Even within the EU, obtaining a license in one member state allows a CASP to operate across the entire Union. This creates the possibility for a CASP to relocate to jurisdictions with light-touch crypto-asset regulation, where licensing and supervision procedures may be less stringent.

This fragmented landscape, with a diversity of regulatory approaches, undermines harmonisation.

5.1.2. Intermediaries

CASPs frequently rely on providers offering integrated payment solutions for cash-in operations. While licensed as EMLs and theoretically subject to AML/CFT obligations, many of these intermediaries remain partially non-compliant and lack sufficient blockchain expertise. Rather than acting as effective gatekeepers, they can increase crypto-asset-related risks.

5.1.3. The regulation of decentralised entities issue

By nature, decentralised finance can make it difficult to locate a protocol's headquarters or identify responsible actors, leaving investigators uncertain about jurisdiction. DeFi protocols and DAOs pose a regulatory challenge – identifying who can be held accountable under AML/CFT obligations.

The FATF clarifies that decentralisation does not remove responsibility when an actor exercises effective control. This includes:

- ▶ Core developers or founders with privileged access;
- ▶ Smart contract administrators;
- ▶ Majority governance token holders; and
- ▶ Commercial entities providing user access to the protocol.

The FATF's functional approach treats any individual or group with sufficient influence over governance or revenues as a virtual asset service provider (VASP), subject to KYC, transaction monitoring, and cooperation obligations⁷¹.

The central issue remains reconciling the ideal of full autonomy promoted by DAOs and DeFi with the regulatory need to identify clear points of accountability to prevent abuse.

Some DeFi platforms have already committed to a less liberal stance, by requesting KYC from their users (e.g. MakerDAO). But these initiatives remain isolated.

The majority of DAOs remain reluctant to take this route, for philosophical, technical and/or business reasons. Overall, the highly decentralised context makes it difficult to ensure that rules are even enforceable.

5.2. Investigations made more complex

5.2.1. Off-chain data

Some transactions escape scrutiny entirely because they are not recorded on the blockchain. Similar to over-the-counter (OTC) transactions on exchanges, certain DeFi protocols move parts of their operations off-chain to increase speed, confidentiality, or scalability. Layer 2 solutions, especially rollups and sidechains, frequently process transactions off-chain to reduce congestion. As a result, only summarised data is recorded on-chain.

71. FATF (2021), "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", October 2021, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

Efficiency comes at the expense of transparency and therefore of investigative capabilities, since investigators may not have complete access to transaction history or details without going through specific Layer 2 block explorers or tools.

Notable examples include:

- ▶ *Hyperliquid* and *dYdX*, leaders in decentralised perpetual trading, which have moved portions of their order books and matching engines off-chain.
- ▶ *Rhino.fi* (formerly DeversiFi), which uses rollups – a technology that compresses transactions into an off-chain batch before recording it on the blockchain.
- ▶ *RenVM (Ren Virtual Machine)*, a decentralised network allowing native assets (BTC, BCH, ZEC) to be transferred to smart contract-compatible blockchains (Ethereum, BSC, and other) while maintaining confidentiality and off-chain compatibility.
 - RenVM operates through a network of nodes called Darknodes, which collectively manage custody of the underlying assets.
 - Users lock their BTC off-chain within RenVM.
 - RenVM issues an equivalent token, renBTC, on Ethereum, which can be used in DeFi applications.
 - Upon withdrawal, renBTC is burned, and RenVM releases the original BTC.
 - In this way, RenVM shifts a critical part of the process – handling deposits, withdrawals, and asset custody – off the Ethereum blockchain, while maintaining transparency and security through distributed consensus among its nodes.

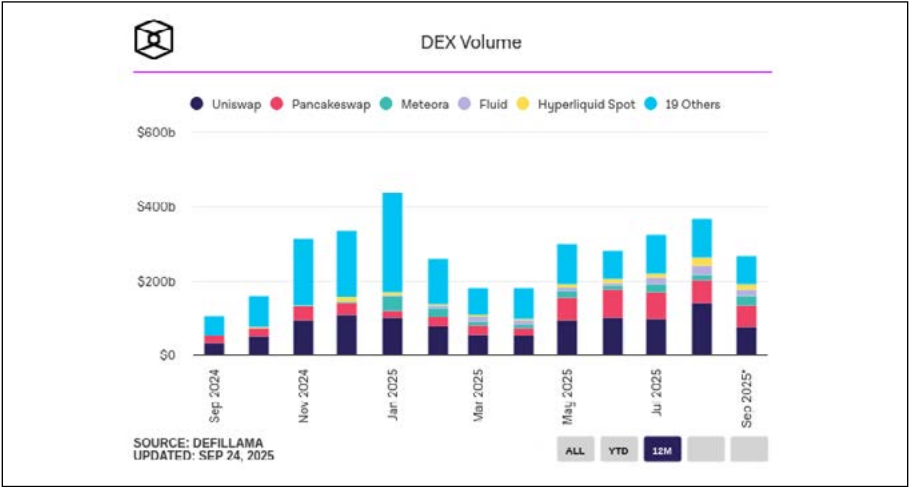
For investigators, accessing off-chain data remains challenging, often requiring cooperation from service providers or access across different jurisdictions.

In addition to the challenges of accessing relevant information, investigators also face:

- ▶ the difficulty of processing large volumes of data, and
- ▶ the extremely high speed of transactions.

5.2.2. Data volume and complexity

The diversity and volume of DeFi operations – swaps, loans, borrowing, staking, and other – are permanently and transparently recorded. In June 2025, monthly DEX volume reached 368 billion US dollars, compared with 1.86 trillion US dollars in spot transactions on crypto exchanges. This sheer volume complicates transaction analysis without specialised tools.



Source: The Block (based on Dune Analytics)⁷²

5.2.3. Velocity

A defining characteristic of DeFi is the speed of execution. Smart contracts operate automatically, often completing transactions almost instantly. Criminal groups can exploit this by automating laundering or using fund-distribution processes, creating chains of transactions that unfold in seconds.

Such fast-moving operations pose significant challenges for financial intelligence units and law enforcement. Money laundering routines may span multiple protocols or services, making flows difficult to trace, while criminals gain a time advantage – disbursing funds before authorities can detect suspicious activity.

This speed makes manual exploitation (using blockchain explorers, for example) very difficult and impractical. Without specialised (free or paid) tools, investigators can very quickly lose track of fraudulent transactions. Methods that were effective just a few years ago are now insufficient due to the sophistication and automation of modern DeFi services.

Specialised monitoring solutions have emerged to address these challenges. Platforms such as TRM Labs, Chainalysis, and Merkle Science Tracker provide real-time on-chain monitoring, capable of triggering alerts based on predefined patterns – similar to a Security Operations Center (SOC) in cybersecurity. Many of these systems now integrate artificial intelligence to enhance detection capabilities.

Despite their effectiveness, these tools remain expensive and are not universally accessible, creating a gap in investigative capabilities across jurisdictions and agencies.

72. Shen T. (2025), “Crypto exchange volume tops \$1.8 trillion in August, highest monthly level since January”, *The Block*, September 2025, accessed 6 October 2025, available at: www.theblock.co/post/369240/crypto-exchange-volume-august

5.2.4. Increasing sophistication and complexity of DeFi products

DeFi introduces innovative financial products and services, but these also add significant complexity to transaction tracing and forensic analysis:

- ▶ *New technological solutions*
 - Some Layer 2 solutions, such as zk-Rollups, incorporate privacy-enhancing technologies (e.g. zk-SNARKs) to enable confidential transactions.
- ▶ *Complex smart contract interactions*
 - *Cross-layer transactions*: Users may move assets multiple times between Layer 1 and Layer 2 before executing a transaction, complicating the tracking of fund flows.
 - *Nested smart contract interactions*: Transactions on Layer 2 may involve multiple smart contracts in a single operation, making it difficult to reconstruct the sequence and purpose of transfers.
- ▶ *Cross-chain interactions*
 - Each blockchain has distinct rules, ledgers, explorers, and indexing methods. Investigations spanning multiple chains require specialised knowledge of each blockchain's structure and behaviour.
 - Forensic analysis tools may not fully support all blockchains, which can limit the ability to trace transactions or link addresses across ecosystems.

5.3. Expertise

Investigating DeFi and crypto-assets requires highly specialised skills and tools. However, investigative authorities worldwide face a persistent shortage of qualified specialists and limited access to advanced blockchain analysis solutions, which are often costly and commercially restricted.

5.3.1. Limited education and training

Investigations involving crypto-assets are typically conducted and monitored by a small pool of specialists within law enforcement, FIUs, or regulatory bodies.

While training opportunities exist, the proportion of staff trained in blockchain and DeFi-related issues remains insufficient compared to the scale of risks and operational needs.

Existing curricula are often general in scope, focusing on blockchain fundamentals and trend analysis, rather than providing hands-on, practice-oriented modules tailored to investigative work.

Advanced training sessions are rare and, when available, tend to be expensive. Many practitioners must rely on in-house training or generic courses that do not address the operational challenges of tracing complex DeFi transactions.

The most comprehensive programs, such as those delivered by Europol's European Cybercrime Centre - EC3 remain limited to a small circle of beneficiaries.

5.3.2. Tooling and crypto-assets tracing

Each blockchain operates under its own technical framework: protocols, transaction structures, consensus mechanisms, and data storage formats. This heterogeneity complicates analysis and demands blockchain-specific expertise.

Traditional databases and surveillance tools used by LEAs and FIUs are poorly adapted for blockchain data analysis and transaction detection, particularly when it comes to DeFi activity.

There is a notable lack of monitoring solutions that can handle cross-chain activity, a growing challenge as criminals increasingly exploit interoperability between blockchains.

In-house expertise is often insufficient to query, interpret, and correlate blockchain data effectively.

5.4. Crypto-assets' recovery: freezing, seizing and managing

Recovering crypto-assets adds a layer of complexity to asset recovery. The speed, novelty and technical complexity of crypto transactions, combined with tracing challenges and cross-border issues, significantly increase the difficulty of recovering proceeds of crime.

5.4.1. Preliminary work

Before any seizure is considered, investigators must precisely identify which crypto-assets constitute proceeds of crime.

Officers who may face crypto-assets seizures should be able to recognise the most relevant traces and artifacts associated with crypto use. Basic awareness should include QR codes, seed phrases, public and private keys, common crypto-assets address formats, and different types of wallets (hardware, software, custodial). Raising this baseline knowledge across law enforcement is essential.

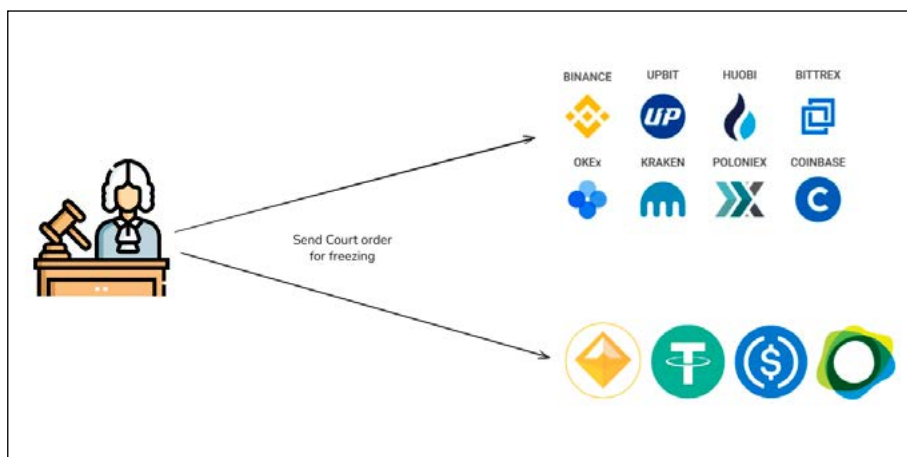
5.4.2. Freezing

Freezing measures are intended to prevent the dissipation of assets that may be returned to victims or forfeited to the state. In practice, freezing requires a judicial order from a competent authority instructing the suspension and blocking of the targeted assets.

When funds are held by a traditional financial institution, this procedure is common and relatively easy to implement. Implementing freezing orders for crypto-assets is more complex than for conventional assets:

- ▶ CASPs (custodial providers): Regulated CASPs that hold customer funds can, in theory, receive and comply with freezing orders. However, their effectiveness is sometimes undermined by the nomadic nature of exchanges: assets may be held in subsidiaries located in non-cooperative jurisdictions or on non-compliant platforms that ignore orders.

- ▶ At a first glance, one might think that crypto-assets deposited in DeFi protocols may be frozen or seized. But the reality is much more nuanced, as stablecoins may be frozen under certain conditions:
 - Issuers of centralised stablecoins (e.g. USDT, USDC) can freeze tokens they have issued and may do so in response to judicial requests.
 - Decentralised stablecoins governed by smart contracts (e.g. DAI) cannot be frozen in the same way because there is no central issuer with control over reserves.



Freezing stablecoins

Stablecoins issuers have the capacity to freeze crypto-assets, but not to seize them.

By using a 'blacklist(address_account)' function embedded in their smart contracts, issuers such as Circle and Tether can blacklist designated addresses, rendering the tokens held in those wallets non-transferable.

This measure can be implemented following the receipt of a court order or when an address is listed by OFAC. Upon receiving a legal request, the issuer verifies that it originates from a competent authority and that it contains the required details – namely, the asset, address and blockchain concerned.

As of September 2025, Tether has blacklisted a total of 1.5 billion tokens across nearly 2 500 addresses, while Circle has banned 358 addresses holding just over 109 million USDC⁷³.

This freezing capability is limited however to primary blockchain and self-custodial wallets. It does not extend to CASPs' deposit addresses, bridges or liquidity pools. Since the private keys remain under the control of the wallet holder, it is technically impossible to seize the frozen funds unless the holder cooperates.

73. See: [USDT and USDC ERC20 Banned Wallets](#), accessed 13 October 2025.

Nevertheless, alternative mechanisms have been developed or are under consideration to help recover funds lost through fraud or hacks:

- ▶ Tether can burn frozen tokens and reissue the equivalent value, thereby recovering funds for victims – as illustrated by the seizure of 225.3 million US dollars by the US Attorney’s Office for the District of Columbia in June 2025⁷⁴.
- ▶ Circle is likewise exploring reversible USDC transactions⁷⁵.

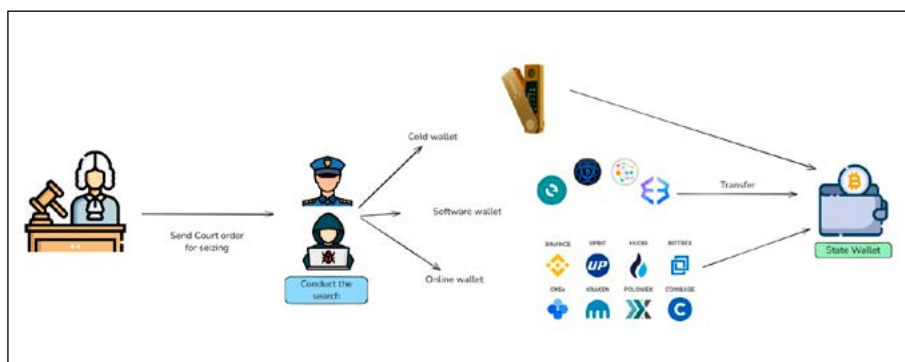
Because freezing normally requires a court order, the process is initiated by national judicial authorities. But FIUs can also play a vital supporting role by detecting suspicious crypto activity and facilitating international cooperation and communication with CASPs as reporting entities.

5.4.3. Seizing

Seizure entails the compulsory transfer of assets into a government-controlled wallet. Depending on the legal framework, the wallet may be controlled by a law enforcement agency, a court, an investigative judge, a public prosecutor, a confiscation body, or a designated asset-management entity.

The pivotal requirement for effective seizure is obtaining control of the private key for the suspect’s wallet. There are two main practical routes:

- ▶ *Via CASPs:* If the assets are held by a custodian, authorities can seek assistance from the relevant CASP – potentially using international cooperation mechanisms – to transfer or freeze the funds.
- ▶ *Directly from the suspect:* If the suspect cooperates (or is compelled), police may obtain the private key or access credentials and transfer funds from a cold wallet (e.g. Ledger), a software wallet (e.g. Electrum, Exodus, MetaMask), or the exchange’s online interface.



74. TRM Labs (2025), “US DOJ Announces Largest Ever Seizure of Funds Related to Crypto Scams”, *TRM Blog. Insights*, June 2025, accessed 13 October 2025, available at: www.trmlabs.com/resources/blog/us-doj-announces-largest-ever-seizure-of-funds-related-to-crypto-scams

75. Hitchcock L. (2025), “Circle Mulls Reversible USDC Stablecoin Transactions in Push for TradFi Adoption”, *decrypt*, September 2025, accessed 16 October 2025, available at: <https://decrypt.co/341374/circle-mulls-reversible-usdc-stablecoin-transactions-in-push-for-tradfi-adoption>

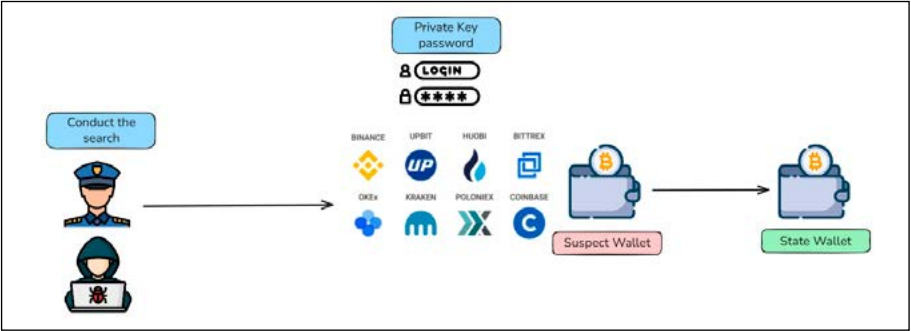
To avoid irreparable mistakes, the operation requires sufficient technical expertise and some basic precautions. It is essential to ensure the accuracy of the destination (public) address. For example, it is advisable to copy and paste the wallet address rather than enter it manually. Careful planning of such an operation is particularly important.

The use of DeFi protocols – via atomic swaps, liquidity pools, cross-chain bridges, automated smart contracts, and mixing services – enables malicious actors to rapidly fragment, move, and anonymise digital assets. This complicates traceability, beneficiary identification, and the effective execution of judicial seizures by law enforcement agencies.

Seizure operations are illustrated more concretely below, focusing on scenarios commonly encountered by investigators.

5.4.3.1. Online wallets

When a suspect uses a custodial wallet, authorities must log in to the platform and transfer the assets to government-controlled wallet. Technical limitations may arise, so tests should be performed before any seizure action. As with traditional banking, adding a new recipient wallet may require a validation delay, which can prolong the transfer to the state-controlled wallet. Two-factor authentication is often required as well, meaning a device (such as a mobile phone) linked to the account must be accessible during the seizure operation.

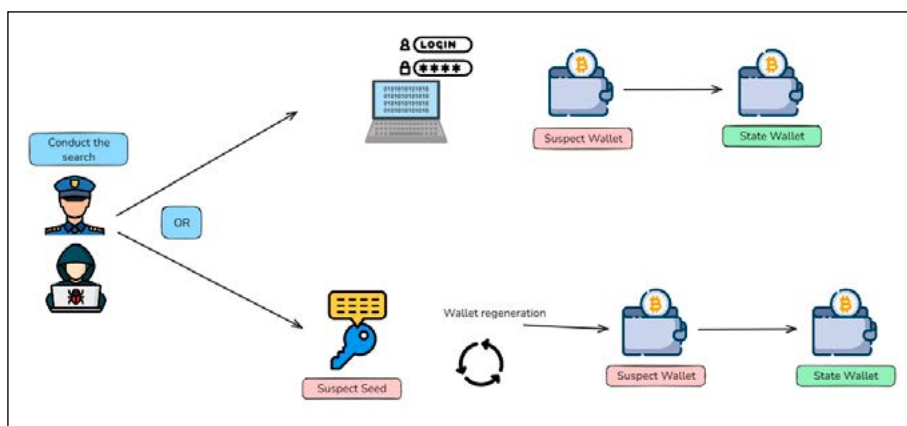


5.4.3.2. Cold wallet

A cold wallet stores private keys on a secured device that is disconnected from the internet making it the safest option against any form of hacking. Two main options enable a transfer from a cold wallet:

- ▶ Knowing the secure device and the access code that protects it (usually a PIN code);
- ▶ Knowing the private key or recovering it from the secret recovery phrase (seed), typically a sequence of 12 or 24 words. This seed regenerates the wallet and enables transfers.

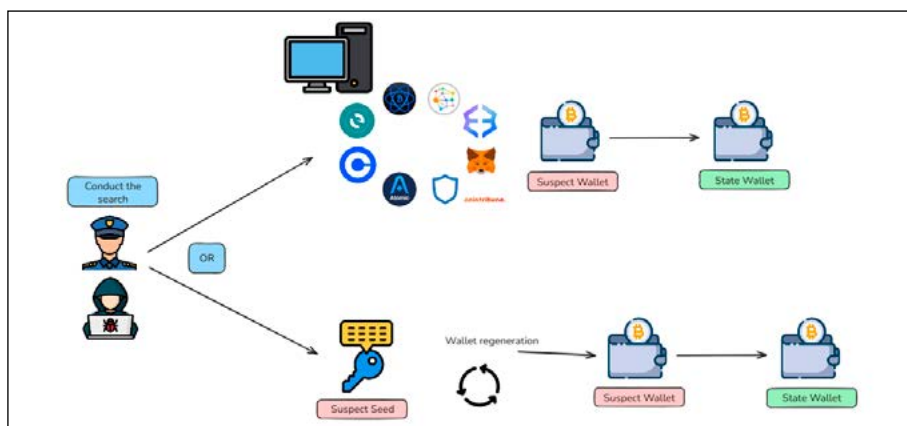
When a seed or cold wallet is found during a search, it is crucial to perform the transfer quickly: an accomplice who also holds the seed can execute a transfer even if police physically possess the cold wallet.



5.4.3.3. Software wallet

In the case of a software wallet (installed on a computer that allows to manage private keys), the situation is similar to the previous one, with the same transfer risks if someone else has the seed.

With a software wallet installed on a computer or device that manages private keys, the risks are similar to those for cold wallets if the seed is known to another party. If someone else has access to the seed or private key, they can transfer funds despite law enforcement control of the device.



5.4.4. Challenges specific to asset recovery

- ▶ The recovery process first requires a clear and specific legal framework.
- ▶ Robust training is essential for front-line officers and investigators to effectively trace and seize assets. They must be able to use blockchain analytic tools and identify crypto-asset information such as private keys or seed phrases. In many countries, despite the growing criminal use of crypto-assets, knowledge among authorities remains limited.

- ▶ Coordination and communication are critical, both with CASPs and foreign counterparts. On the requesting side, orders must be drafted correctly, using accurate terminology and details (e.g. deposit addresses). On the receiving side, adequate human resources and technical expertise are needed to respond in a timely manner, especially in jurisdictions hosting numerous or major exchanges.
- ▶ The management of seized crypto-assets presents specific challenges, such as volatility.

The adaptability of illicit networks, combined with the criminals' evolving tactics, underscores the need for continuous vigilance and close cooperation between regulators, law enforcement agencies, and private sector stakeholders.

5.5. International cooperation

The fight against illegal activities involving crypto-assets and DeFi abuse increasingly relies on international cooperation. Criminal activities in this domain are inherently transnational, as services, infrastructure, and actors often span multiple jurisdictions.

Numerous initiatives already exist and are led by international organisations such as the United Nations Office on Drugs and Crime (UNODC) the Council of Europe, Europol, Interpol, the European Union, the Organisation for Security and Co-operation in Europe and the Egmont Group of Financial Intelligence Units.

These frameworks enable:

- ▶ information sharing (e.g. suspicious indicators, typologies, case studies);
- ▶ development of best practices and investigative methodologies;
- ▶ harmonisation of approaches to improve collective resilience;
- ▶ capacity-building and training for intelligence services and law enforcement agencies.

Europol, for example, supports EU member states in the fight against serious crime and terrorism. It relies on specialised analysts and hosts databases of indicators of compromise provided by national authorities.

Nonetheless, cooperation on crypto-asset cases still faces obstacles at the operational level, often due to limited expertise, insufficient resources, and a lack of coordination.

5.5.1. Channels of cooperation

Cross-border cooperation on crypto-assets can occur through multiple channels:

- ▶ *FIU-to-FIU cooperation*: FIUs exchange financial intelligence on ML/TF cases via the Egmont Secure Web. This includes incoming requests for information (and corresponding replies) as well as spontaneous intelligence sharing. One distinctive strength of this network is its ability to exchange information rapidly and securely, which can sometimes compensate for the slowness of mutual legal assistance procedures. At the EU level, FIU.net provides a secure and decentralised platform shared by Member States, Iceland, Liechtenstein, Norway, Europol, and the Egmont Group. It facilitates the communication of

ML cases and enables automated cross-border reporting and queries (including a “match” function to check whether an individual or entity is already known to another FIU).

However, the quality of exchanges involving crypto-assets remains uneven, reflecting the very different levels of expertise among FIUs. Moreover, there is no direct correlation between the size of a country’s CASP industry and the volume of intelligence exchanges with its FIU: jurisdictions licensing major exchanges may still lack the legal powers, resources, or willingness to share information. Unlike Europol for police forces, there is no equivalent structure to carry out joint strategic or operational analysis for FIUs.

- ▶ *Police-to-police cooperation:* Police forces can cooperate directly, for instance via Europol’s Secure Information Exchange Network Application (SIENA) messaging system or through the 24-hour contact points available under the Budapest Convention on Cybercrime⁷⁶.
- ▶ *Judicial cooperation:* Courts and prosecutors exchange information through European Mutual Assistance Requests or International Criminal Cooperation Requests. These instruments allow evidence gathering, extradition, and coordination in cross-border prosecutions.

However, timelines for requests involving crypto-assets are often lengthy, depending on the maturity of the requested country’s legal framework and the efficiency of its international cooperation mechanisms. Authorities also note the persistence of non-cooperative jurisdictions, such as the Seychelles, where several major exchanges are licensed (e.g. Binance, Bybit, HTX, Kucoin).

In addition to these official channels, authorities may rely on informal cooperation, leveraging professional networks and goodwill. This is particularly relevant in the blockchain sector, which often transcends national frameworks. Informal exchanges can involve both foreign authorities and CASPs. In practice, direct contacts with centralised exchanges – or even with decentralised exchanges, provided an identifiable administrator exists – can yield valuable technical, legal, or financial information. Such cooperation can support ongoing investigations, facilitate seizures, and prepare the ground for subsequent formal requests.

76. [About the Convention - Cybercrime](#)

6. Good practices and recommendations

6.1. Regulatory framework

The rapid evolution of the DeFi ecosystem makes it difficult for regulations to keep pace, with new rules often becoming quickly unsuitable or outdated. As a result, most legal frameworks still rely on existing obligations for centralised intermediaries, focusing primarily on KYC/AML requirements and investor protection.

The democratisation of DeFi must necessarily be accompanied by broader regulation and supervision that take into account its specific features – particularly its anonymity and absence of intermediaries. Striking an appropriate balance between promoting innovation and mitigating the potential risks and negative impacts of DeFi could build upon the following areas of focus:

- 1) At the national level, adapt existing legal frameworks to effectively incorporate new technological features linked to DeFi or, where such frameworks do not exist, develop dedicated legislation. This should include clear and detailed guidelines on the definition of CASPs, the enforcement of AML/CFT requirements, the issuance of crypto-assets, and their taxation. It should also be tailored to each country's specific context, taking into account factors such as market size, the level of digital adoption and usage, technological maturity, and the broader legal environment.
- 2) Seek to establish a harmonised approach and adopt global standards to prevent jurisdictional arbitrage and the emergence of “crypto havens”.
- 3) Create regulatory sandboxes (safe spaces for innovative financial institutions and technology-driven activities) to allow testing of projects and refining of products in a controlled environment before their public launch.
- 4) Consider legal liability and accountability for protocol developers, DAO members, and other incentivised parties, including the possibility of registering DAOs as legal entities when certain conditions are met.
- 5) Establish a legal framework for smart contracts, including certification and validation rules to ensure transparency, security, and enforceability.

6.2. Continuous monitoring

It is essential to continuously monitor the crypto ecosystem in order to keep track of its evolution, identify new CASPs that may be subject to licensing, understand emerging products and technical developments, assess the level of public adoption of crypto-assets, and evaluate their potential misuse by criminal groups.

The ban on the use of crypto-assets in some countries should not be viewed as an obstacle. Given the ease of access to crypto-assets, it is very likely that a portion of the population continues to use them regardless of the national legal framework.

In such a constantly evolving industry, numerous resources can help to stay up to date – ranging from general information (press and online resources) to more operational and technical sources (academic literature, dedicated forums such as GitHub, and social media). These can be leveraged by countries to better assess the ML risk associated with crypto-assets and CASPs.

Crypto-assets and National Risk Assessment (NRA)

Under the FATF Standards, countries are required to understand the ML/TF risks associated with crypto-assets, identify the natural and legal persons conducting VASP activities, and supervise the sector in the same manner as financial institutions.

As of April 2025, less than one-third (29%) of jurisdictions were assessed as compliant or largely compliant with the amended Recommendation 15 (41 out of 138 jurisdictions assessed)⁷⁷.

In accordance with Recommendations 1 and 15, crypto-asset risks should be integrated into each jurisdiction's NRA, and mitigation measures should be implemented following a risk-based approach. Countries may refer to the *Quick Guide with Suggested Areas for Assessing the ML Risks Linked to VA/VASPs* (FATF, June 2025⁷⁸) and to the *FATF 2021 Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*⁷⁹.

Recommendations:

- ▶ Promote regular exchanges between crypto practitioners, ideally coordinated by a central body responsible for the NRA.
- ▶ Involve all relevant stakeholders – supervisors, law enforcement and FIUs, judicial authorities, and reporting entities (including CASPs) – in the risk assessment process.
- ▶ Identify intersections or convergence points between DeFi, CeFi, and TradFi.
- ▶ Conduct studies on DAOs to determine evidence suggesting the presence of a centralised structure.

77. FATF (2025), *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, June 2025, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

78. FATF, *Quick guide on assessing the Money Laundering risks of virtual assets (VA) and virtual asset service providers (VASP)*, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Methodsand Trends/quick-guide-on-assessing-ML-risks-of-VA-and-VASPs.html

79. FATF (2021), *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, October 2021, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

6.3. Education and training

Specialised training for investigators and analysts is an essential prerequisite to raise awareness of the subject matter, to help them initiate basic investigations, and to develop operational expertise for complex cases.

However, knowledge of the crypto ecosystem should not be limited to investigative units alone. It must extend across the entire financial intelligence chain, including judicial authorities, regulators, and the full chain of command.

This outreach can take two directions:

- ▶ Increasing general understanding of crypto-assets and services is essential to strengthen the overall response to financial crime.
- ▶ Developing technical expertise is equally important to enable specialists to efficiently tackle organised crime and money laundering.

There is an extensive range of education and training opportunities related to crypto-assets. While the variety may seem confusing at first, this diversity can meet the needs of learners at all levels.

- ▶ *Open sources* include dedicated books, websites, forums, podcasts, and social networks that provide sufficient knowledge to become proficient and begin basic investigations. Several universities also offer Massive Open Online Courses, such as the University of Nicosia's courses on blockchain, digital assets, and DeFi⁸⁰.
- ▶ *International bodies and organisations* have addressed blockchain-related issues for several years – including the Basel Institute, European Union Agency for Law Enforcement Training (CEPOL), the Council of Europe, the Egmont Group (ECOFEL), Europol, Interpol, the Organisation for Economic Co-operation and Development, and UNODC. Some of them offer dedicated capacity-building and training programmes.
- ▶ *Reports and publications*:
 - General reports published by blockchain analytics companies (e.g. Elliptic), blockchain security providers (e.g. Blocksec), international organisations, FIUs, and LEAs provide valuable information on typologies and emerging trends. They often contain insights that can complement local strategic analyses.
 - Software vendors and cybersecurity firms regularly publish reports presenting new trends or detailing investigative processes. These publications are another valuable resource for those seeking to better understand and investigate these phenomena.
- ▶ *Commercial providers* (e.g. blockchain analytics companies) naturally offer training courses alongside the purchase of software licences. These courses are generally well-structured, certified, and tailored to different user levels. However, they focus exclusively on a single proprietary tool, increasing the risk of dependency. Such training should therefore be reserved for investigators who will use the tool regularly or who manage complex investigations.

80. See: [Mastering Web3: Blockchain, Cryptocurrencies, NFTs, and the Metaverse - University of Nicosia](#)

Most of these resources focus on the fundamentals of blockchain and are useful for deepening understanding of the topic. However, training sessions aimed at specialists seeking to significantly enhance their skills remain limited and/or expensive. The Europol European Cybercrime Centre is recognised as a centre of excellence for crypto investigations, but its training programmes are restricted to police forces and are generally not accessible to experts from non-police FIUs, judicial authorities, or supervisory bodies.

Building a layered training approach – combining broad introductory courses, targeted tool-based sessions, and continuous self-learning through open resources – remains the most effective way to develop sustainable expertise.

Recommendations:

- ▶ Establish a continuous training framework that brings together all relevant stakeholders (investigative, analytical, and asset recovery services, judicial authorities, regulators) in order to create a common training foundation and share best practices.
- ▶ Develop a tiered training programme offering tailored sessions adapted to the specific needs and resources (human, technical, and financial) of each agency or department.
- ▶ Prioritise open source resources over paid solutions, as they provide a solid foundation for developing basic expertise and conducting initial investigations.
- ▶ Extend basic training to a wider range of staff, including the chain of command.
- ▶ Establish a group of advanced experts from various agencies to share specific investigative techniques and knowledge of analytical tools. They could then provide in-house training (Training of Trainers) to their colleagues.

These efforts should ideally be part of a broader initiative involving the general public, aimed at raising global awareness of the challenges and risks associated with the use of crypto-assets. One objective is to reduce the threats posed by the growing number of crypto-related scams.

6.4. Investigating capacity

Analysts and investigators still tend to work in isolation, often using inadequate tools. Frequently confronted with the same challenges – analysing CASP files, understanding technical transactions, or tracing assets through bridges or mixers – they often manage to find solutions independently, while experts in other departments or agencies face similar difficulties. To save time and avoid duplication of effort, it is essential to pool resources and expertise as much as possible.

The objective is to improve the detection, tracing, analysis, and reporting of cases involving crypto-assets and DeFi.

- ▶ Properly detecting traces of crypto-assets is a prerequisite – whether to initiate analysis, prepare a house search, or consider a seizure. This task should not be limited to experts alone but should involve all stakeholders, from compliance units in reporting entities to judicial authorities. Outreach efforts are therefore

necessary and could lead to the creation of a catalogue listing key indicators and red flags for identifying crypto-asset activity (e.g. typical crypto address formats, related IBANs, seed phrases, and other).

- ▶ As described above, analytical work is further complicated by the volume and complexity of transactions, which may involve multiple assets, blockchains, and/or smart contracts. Tools provided by blockchain analytics companies can assist in certain investigations, but their coverage is uneven – some blockchains remain unsupported or only partially visible. While most blockchain data is publicly accessible, its operational use requires efficient mass data processing capabilities.

Specific investigative guides have been developed at both national and international levels, but they often remain confidential or underutilised.

Recommendations:

- ▶ Develop efficient methods to report and communicate findings clearly.
- ▶ Establish or update specific standard operational procedures (SOPs), such as financial profiling, investigative, and asset recovery guides.
- ▶ Pool resources to acquire and share specialised investigative tools for crypto and blockchain analysis.
- ▶ Create dedicated teams for complex investigations composed of officers with strong OSINT and financial innovation skills, and ideally, an interest in understanding computer code.
- ▶ Explore and develop automation and AI-powered tools to support the detection and analysis of blockchain data.

6.5. National cooperation

Coordination at the national level can help better allocate resources and avoid duplication of efforts. Several good practices can be highlighted:

- ▶ More advanced units can share their experience – and lessons learnt – with less experienced agencies (e.g. identifying contact points within CASPs, tracing through bridges, or understanding new typologies).
- ▶ Encourage regular exchanges between stakeholders (LEAs, FIUs, judicial authorities and CASPs) in order to facilitate and speed up investigations and proceedings. This cooperation is particularly important when dealing with complex cases (e.g. large-scale scams, ransomware, and other), or freezing crypto-assets. Such exchanges can also enable to better grasp CAPSs and other DeFi players' peculiarities.

Recommendations:

- ▶ Clarify communication formats between law enforcement authorities, FIUs, judicial authorities, and CASPs.
- ▶ Encourage the pooling of knowledge and the sharing of best practices at the national level, through light coordination structures bringing together key experts from investigative units of the police, customs, tax administration, FIUs, and the judiciary.

- ▶ Prioritise joint procurement of blockchain tracing software, with the dual aim of reducing costs and promoting interoperability across agencies.

6.6. Asset seizure, recovery and management

Efficient procedures must be established to ensure rapid and effective action within a short timeframe. Considering the many challenges previously mentioned – legal frameworks, technical skills, training needs, and the requirement for efficient communication – specific guidance on asset recovery is necessary.

In addition to specialised training, these guidelines should include clear rules on:

- ▶ Pre-planning procedures;
- ▶ Creation and management of government-controlled wallets;
- ▶ Post-seizure asset management.

A comprehensive guidance should necessarily encompass the specificities of DeFi, with stablecoins in particular.

Several practical guides already exist, including the *Guide on Seizing Cryptocurrencies* published by the Council of Europe in 2021⁸¹, which could serve as a basis (though it would benefit from an update).

Recommendations:

- ▶ Draft specific legislation on crypto-asset seizure.
- ▶ Establish practical guidance detailing how to identify, freeze, seize, and manage crypto-assets.
- ▶ Integrate crypto-asset aspects into existing asset recovery training modules.

6.7. International cooperation

The international dimension plays a crucial role in the ever-changing crypto ecosystem, where new actors constantly emerge, and others engage in jurisdictional arbitrage. The main challenges lie in obtaining information – mostly from CASPs – in a timely manner and ensuring the effective exchange of intelligence with foreign counterparts. While some initiatives have been undertaken, they remain insufficient:

- ▶ Mapping the location of CASPs, along with analysing the content of received files, facilitates the submission of requests and helps identify loopholes (such as non-compliant CASPs or unresponsive jurisdictions). A few initiatives, such as the Egmont list of CASPs, have been developed, but they remain isolated, lack regular updates, and are often inaccessible.
- ▶ Sharing intelligence with foreign counterparts still too often encounters obstacles due to limited knowledge of crypto-related cases, where precise and accurate terminology is essential. This significantly hampers the quality and

81. Council of Europe (2021), "*Guide on seizing cryptocurrencies*", February 2021, accessible to registered users only of the Council of Europe's CYBOX online platform for exchange, training, and resource sharing on cybercrime and electronic evidence, accessible at: [Home | CYBOX](#).

speed of exchanges. On the one hand, requesting authorities must be able to narrow down their queries using appropriate terms (e.g. transaction hash or deposit address). On the other hand, requested units – especially those in jurisdictions hosting numerous or major CASPs – must be able to understand and process these requests effectively.

- ▶ Complex crypto-related investigations generally involve several jurisdictions, but the velocity of DeFi transactions contrasts sharply with the slowness of international cooperation procedures. Crypto-assets can move across exchanges located in multiple countries within minutes, whereas formal requests may take weeks to be processed. There is an urgent need to consider faster and more operational mechanisms for information exchange. The newly established AMLA could draw inspiration from Europol's successful operational models.

In addition, informal cooperation can effectively complement traditional channels of international cooperation. This applies equally to public-public and public-private exchanges. Informal coordination can help mitigate the slowness of formal procedures and facilitate smoother collaboration.

For instance, early informal cooperation in support of an MLA request can enable faster coordination and prioritisation. It also allows investigators to refine their formal requests by focusing on specific wallets (e.g. those showing unusual activity or positive balances).

Recommendations:

- ▶ Establish and regularly update a global mapping of CASP registrations and licences, based on jurisdictions' contributions, indicating for each major CASP which branch, or subsidiary serves clients from specific jurisdictions.
- ▶ Ensure that units responsible for international cooperation can efficiently handle requests and responses involving crypto transactions.
- ▶ Encourage operational cross-border initiatives – bilateral or multilateral – such as those led by Europol and leverage the forthcoming AMLA as an opportunity to strengthen these mechanisms.
- ▶ Foster informal cooperation to complement formal exchanges and improve responsiveness.

6.8. Public-private cooperation

Collaboration between public authorities (FIUs, LEAs, tax authorities, prosecutors, and supervisors) and the private sector (notably reporting entities) can significantly strengthen investigative and prosecutorial capabilities.

Public-private cooperation is promoted in the new AML package through:

- ▶ A dedicated provision on the *"exchange of information within partnerships for information sharing"*⁸²;

82. Article 75 of the [Regulation \(EU\) 2024/1624](#), accessed 15 September 2025

- ▶ The possibility for the new Anti-Money Laundering Authority to “*set up cross-border partnerships for information sharing and to participate in partnerships established in one or across several Member States*”⁸³.

This approach is also encouraged by various international institutions such as the FATF, Interpol, and the Egmont Group⁸⁴.

Public-private collaboration can bring substantial added value by supporting ongoing criminal investigations, improving asset recovery, and deepening the understanding of emerging risks. Examples include:

- ▶ Enhancing understanding of CASP services and products (e.g. automated market makers) and their technical implications – an essential step for interpreting complex transaction histories.
- ▶ Improving the identification and collection of relevant data through enhanced communication. Financial institutions can assist in pinpointing useful information within vast datasets and, in return, benefit from higher-quality suspicious transaction reports.
- ▶ Identifying new investigative leads by promptly sharing newly detected typologies, thereby enabling both LEAs to uncover new cases and reporting entities to fine-tune their monitoring systems.
- ▶ Strengthening and accelerating asset-freezing and seizure mechanisms through better coordination.

The Europol Financial Intelligence Public-Private Partnership (EFIPPP⁸⁵) is one example of a collaborative platform that promotes such exchanges and operational cooperation.

Recommendations:

- ▶ Join or establish public-private initiatives that enable regular exchanges for both operational and strategic analysis.
- ▶ Consider maintaining informal contacts with CASPs for guidance, identification of new cases, and potential assistance with asset seizures.

83. Article 93 of the [Regulation \(EU\) 2024/1620](#), accessed 15 September 2025

84. FATF - Egmont Group - Interpol - UNODC (2025), “*International Co-operation on Money Laundering Detection, Investigation, and Prosecution Handbook*”, accessed 6 October 2025, available at: <https://www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html>. See also at the same link three brochures on “*Effective informal operational and strategic information exchange*” – A practical guide for FIUs, A practical guide for LEAs and “*Enhancing AML/CFT investigations through informal international co-operation*” – A practical guide for central authorities in charge of MLA, including prosecutors (prepared by Egmont Group, FATF, Interpol and UNODC).

85. See: <https://efipp.eu/>, accessed 26 September 2025

7. Bibliography

7.1. Legal and Regulatory Texts

The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols: [About the Convention - Cybercrime](#)

Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010: [Regulation \(EU\) 2024/1620](#)

Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: [Regulation \(EU\) 2024/1624](#)

Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849: [Directive \(EU\) 2024/1640](#)

Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849: [Regulation - 2023/1113 - EN - EUR-Lex](#)

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937: [Regulation \(EU\) 2023/1114](#)

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC: [Directive - 2009/110 - EN - EUR-Lex](#)

Guiding and Establishing National Innovation for U.S. Stablecoins Act” or the “GENIUS Act”: [Text - S.1582 - 119th Congress \(2025-2026\): GENIUS Act | Congress.gov | Library of Congress](#)

7.2. Institutional reports and publications

Council of Europe (2021), *“Guide on seizing cryptocurrencies”*, February 2021, accessible to registered users only of the Council of Europe’s CYBOX online platform for exchange, training, and resource sharing on cybercrime and electronic evidence, accessible at: [Home | CYBOX](#).

ESMA (2024), Public Statement *“On the provision of certain crypto-asset services in relation to non-MiCA compliant ARTs and EMTs”*, January 2025, accessed 16 October 2025, available at: www.esma.europa.eu/sites/default/files/2025-01/ESMA75-223375936-6099_Statement_on_stablecoins.pdf

ESMA (2023), Consultation Paper *“Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) - second consultation paper”*, October 2023, accessed 16 October 2025, available at: www.esma.europa.eu/sites/default/files/2023-10/ESMA75-453128700-438_MiCA_Consultation_Paper_2nd_package.pdf

ESMA (2023), *“Decentralised Finance in the EU: Developments and risks”*, October 2023, accessed 16 October 2025, available at: www.esma.europa.eu/sites/default/files/2023-10/ESMA50-2085271018-3349_TRV_Article_Decentralised_Finance_in_the_EU_Developments_and_Risks.pdf

European Central Bank (2023), *“The Future of DAOs in Finance: in Need of Legal Status”*, October 2023, accessed 16 October 2025, available at: www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf

European Parliament (2023), *“Remaining regulatory challenges in digital finance and crypto-assets after MiCA”*, April 2023, accessed 16 October 2025, available at: [www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2023\)740083](http://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2023)740083)

Europol (2024), *“Crackdown on money mule service providers laundering over EUR 10 million”*, May 2024, accessed 6 October 2025, available at: www.europol.europa.eu/media-press/newsroom/news/crackdown-money-mule-service-providers-laundering-over-eur-10-million

Europol (2023), *“One of the darkweb’s largest cryptocurrency laundromats washed out”*, March 2023, accessed 6 October 2025, available at: www.europol.europa.eu/media-press/newsroom/news/one-of-darkwebs-largest-cryptocurrency-laundromats-washed-out

FATF (2021), *“Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers”*, October 2021, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

FATF (2025), *“Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers”*, June 2025, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

FATF – Egmont Group – Interpol – UNODC (2025), *“International Co-operation on Money Laundering Detection, Investigation, and Prosecution Handbook”*, accessed 6 October 2025, available at: www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html

See also at the same previous link three brochures on “Effective informal operational and strategic information exchange” – A practical guide for FIUs, A practical guide for LEAs and “Enhancing AML/CFT investigations through informal international co-operation” – A practical guide for central authorities in charge of MLA, including prosecutors (prepared by Egmont Group, FATF, Interpol and UNODC).

UNODC (2024), “Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat”, January 2024, accessed 6 October 2025, available at: <https://www.unodc.org/roseap/en/2024/casinos-casinos-cryptocurrency-underground-banking/story.html>

US Department of the Treasury (2025), “Illicit Finance Risk Assessment of Decentralized Finance”, April 2023, accessed 16 October 2025, available at: <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

World Economic Forum (2024), “Digital Assets Regulation: Insights from Jurisdictional Approaches”, October 2024, accessed 16 October 2025, available at: www.weforum.org/publications/digital-assets-regulation-insights-from-jurisdictional-approaches/

7.3. Academic and research

Brownworth A. et al. (2024), “Regulating decentralized systems: evidence from sanctions on Tornado Cash”, *SNB Working Papers*, September 2024, accessed 6 October 2025, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4930935

Roul A. (2024), “The Rise of Monero: ISKP’s Preferred Cryptocurrency for Terror Financing”, Global Network on extremism and technology, October 2024, accessed 6 October 2025, available at: <https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/>

Trozzea A. et al. (2023), “Of Degens and Defrauders: Using Open-Source Investigative Tools to Investigate Decentralized Finance Frauds and Money Laundering”, May 2023, accessed 16 October 2025, available at: <https://arxiv.org/abs/2303.00810>

Carpentier-Desjardins C. et al. (2025), “Mapping the DeFi crime landscape: an evidence-based picture”, *Journal of Cybersecurity*, Volume 11, Issue 1, 2025, Cornell University, January 2025, accessed 6 October 2025, available at: <https://arxiv.org/abs/2310.04356>

Schär F. (2021), “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets”, Federal Reserve Bank of St. Louis Review, Second Quarter 2021, accessed 6 October 2025, format PDF, available at: www.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

Furneaux N. (2024), “There’s No Such Thing as Crypto Crime: An investigative handbook”, Wiley Editions.

Mafrur R. (2025), “Blockchain Data Analytics: Review and Challenges”, Department of Applied Finance, Macquarie University, Australia, August 2025, accessed 16 October 2025, available at: <https://arxiv.org/pdf/2503.09165>

7.4. Press and news articles

Robertson A. (2022), "Hackers and fraudsters used crypto bridge RenBridge to launder \$540 million, says report/ Including Russian and North Korean operations", *The Verge*, August 2022, accessed 6 October 2025, available at: www.theverge.com/2022/8/10/23299841/crypto-bridge-renbridge-used-launder-money-russia-north-korea-ransomware-report

Shumba C. (2024), "Duo Behind \$9M Platypus Exploit Acquitted by Paris Court: Report", *CoinDesk*, March 2024, accessed 6 October 2025, available at: www.coindesk.com/policy/2023/12/04/duo-behind-9m-platypus-exploit-acquitted-by-paris-court-report

Omelchenko D. (2025), "Managed DeFi Yield Provider Tesseract Secures MiCA License", *The Defiant*, September 2025, accessed 6 October 2025, available at: <https://thedefiant.io/news/defi/defi-yield-provider-tesseract-mica-license>

Patairya D. K. (2023), "Crimeware-as-a-service: A new threat to crypto users", *Cointelegraph*, January 2025, October 2023, accessed 6 October 2025, available at: <https://cointelegraph.com/explained/crimeware-as-a-service-a-new-threat-to-crypto-users>

Hitchcock L. (2025), "Circle Mulls Reversible USDC Stablecoin Transactions in Push for TradFi Adoption", *decrypt*, September 2025, accessed 16 October 2025, available at: <https://decrypt.co/341374/circle-mulls-reversible-usdc-stablecoin-transactions-in-push-for-tradfi-adoption>

Chipolina S. (2023), "Cryptocurrencies play 'endemic role' in organised crime", *Financial Times*, October 2023, accessed 6 October 2025, available at: www.ft.com/content/378a05ac-a12b-41f9-a80c-fc79a36bc44b

Gallagher S. (2024), "Cryptocurrency scams metastasize into new forms", *Global Network on extremism and technology*, October 2024, accessed 6 October 2025, available at: <https://news.sophos.com/en-us/2024/02/02/cryptocurrency-scams-metastasize-into-new-forms/>

Shen T. (2025), "Crypto exchange volume tops \$1.8 trillion in August, highest monthly level since January", *The Block*, September 2025, accessed 6 October 2025, available at: www.theblock.co/post/369240/crypto-exchange-volume-august

7.5. Professional / Corporate / Technical Sources

Blocksec (2024), "#5: Platypus Finance: Surviving Three Attacks with a Stroke of Luck", February 2024, accessed 13 October 2025, available at: <https://blocksec.com/blog/5-platypus-finance-surviving-three-attacks-with-a-stroke-of-luck>

Chainalysis (2025), "*The Chainalysis 2025 Crypto Crime Report*", accessed 6 October 2025, available at: www.chainalysis.com/blog/2025-crypto-crime-report-introduction/

Cyberscope (2024), "*Drainer-as-a-Service (DaaS): Unmasking the Dark Web's Latest Threat*", November 2024, accessed 13 October 2025, available at: <https://cyberscope.medium.com/drainer-as-a-service-daas-unmasking-the-dark-webs-latest-threat-e54ad69d12da>

Dune and Artemis (2025), “*The State of Stablecoins 2025: Supply, Adoption & Market Trends*”, accessed 3 October 2025, available at: <https://dune.com/stablecoin-download>

Elliptic (2025), “The state of cross-chain crime 2025”, *Elliptic Report*, accessed 16 October 2025, available at: www.elliptic.co/resources/the-state-of-cross-chain-crime-2025

Elliptic (2025), “Xinbi: The \$8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers”, *Elliptic Research*, May 2025, accessed 6 October 2025, available at: www.elliptic.co/blog/xinbi-guarantee?utm_source

Elliptic (2025), “The largest theft in history following the money trail from the Bybit Hack”, *Elliptic Research*, February 2025, accessed 10 December 2025, available at: www.elliptic.co/blog/bybit-hack-largest-in-history

Immunefi (2023), “Medium - Hack Analysis: Platypus Finance”, *Medium*, February 2023 (18 April 2023), accessed 16 October 2025, available at: <https://medium.com/immunefi/hack-analysis-platypus-finance-february-2023-d11fce37d861>

IOSCO (2022), “*Decentralized Finance Report*”, March 2022, accessed 6 October 2025, available at: www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf

Mihajlović M. (2023), “A Guide to Crypto Twitter”, *Shrimpy Academy*, May 2023, accessed 6 October 2025, available at: <https://web.archive.org/web/20250327071713/https://academy.shrimpy.io/post/a-guide-to-crypto-twitter>

Merkle Science (2024), “*Understanding Regulatory Frameworks for DeFi in the U.S. and Beyond*”, June 2024, accessed 16 October 2025, available at: www.merklescience.com/blog/understanding-regulatory-frameworks-for-defi-in-the-u-s-and-beyond

Nansen (2022), “*Nansen adds ERC1155 support for NFTs*”, February 2022, accessed 15 October 2025, available at: www.nansen.ai/post/nansen-adds-erc1155-support-for-nfts

Latka N. (2024), “Is DeFi Truly Exempt from MiCA Regulations?”, *Merkle Science*, June 2024, accessed 16 September 2025, available at: www.merklescience.com/blog/is-defi-truly-exempt-from-mica-regulations

Behnke R. (2022), “Explained: The Ronin Hack – March 2022”, *Halborn*, March 2023, accessed 6 October 2025, available at: www.halborn.com/blog/post/explained-the-ronin-hack-march-2022?utm_source=chatgpt.com

Gherhelas S. (2025), “Dapp Industry Report 2024 Overview”, January 2025, *DappRadar*, accessed 16 October 2025, available at: <https://dappradar.com/blog/dapp-industry-report-2024-overview>

TRM Labs (2023), “Best practices for digital asset seizures”, *TRM Blog. Insights*, June 2023, accessed 16 October 2025, available at: www.trmlabs.com/resources/blog/best-practices-for-digital-asset-seizure-in-the-field

TRM Labs (2025), “US Law Enforcement Dismantles \$24M Dark Web Crypto Laundering Network”, *TRM Blog. Insights*, April 2025, accessed 6 October 2025, available at: www.trmlabs.com/resources/blog/us-law-enforcement-dismantles-24m-dark-web-crypto-laundering-network

TRM Labs (2025), "US DOJ Announces Largest Ever Seizure of Funds Related to Crypto Scams", *TRM Blog. Insights*, June 2025, accessed 13 October 2025, available at: www.trmlabs.com/resources/blog/us-doj-announces-largest-ever-seizure-of-funds-related-to-crypto-scams

Tiwari V. (2025), "GENIUS Act Passes: What 2025's Stablecoin Bill Means for Issuers & Banks", *Merkle Science*, June 2025, accessed 16 October 2025, available at: www.merklescience.com/blog/genius-act-passes-what-2025s-stablecoin-bill-means-for-issuers-banks

8. List of resources and tools

Name	Link	Description
A. Blockchain explorers and analytics		
Arkham	https://arkhamintelligence.com https://intel.arkm.com/	Open source blockchain explorer
Bitquery	https://bitquery.io https://explorer.bitquery.io/	Blockchain data provider and explorer
Blockchain.com	https://www.blockchain.com	BTC blockchain explorer
Blockchair	https://blockchair.com	Multichain explorer
Blockscout	https://www.blockscout.com/	Multichain explorer
Breadcrumbs	https://www.breadcrumbs.app/	Blockchain analytics platform
BSC Scan	https://bscscan.com/	BNB smart chain explorer
Caudena (ex Clain)	https://caudena.com	
Debank	https://debank.com/	Portfolio tracker for ETH and EVM
Dune	https://dune.com	Blockchain analytics
Etherscan	https://etherscan.io	Ethereum blockchain explorer
Ethplorer	https://ethplorer.io	Ethereum tokens explorer
Footprint Analytics	https://www.footprint.network	Blockchain analytics platform
Mempool	https://mempool.space/	Bitcoin (BTC) blockchain explorer
OP-Etherscan	https://optimistic.etherscan.io/	Optimism blockchain explorer
Oklink	https://www.oklink.com/fr	Multichain explorer
Solcan	https://solscan.io/	Solana (SOL) blockchain explorer
Tronscan	https://tronscan.org	Tron (TRX) blockchain explorer
Wallet Explorer	https://www.wallexplorer.com/	Bitcoin (BTC) blockchain explorer
B. Other useful links		
Blocksec - Metasleuth	https://metasleuth.io/	Valuable open source toolkit
Blocksec - Metasuites	https://blocksec.com/metasuites	
BubbleMaps	https://bubblemaps.io/	Data visualisation platform
Chainabuse	https://chainabuse.com/	Global reporting platform on crypto scams
CryptoscamDB	https://cryptoscamdb.org/scams	Open source dataset tracking malicious URLs
DappRadar	https://dappradar.com/	Tracking and ranking dApps
DeepDAO	https://deepdao.io	Analytics tool for the DAO ecosystem

Name	Link	Description
ENS	https://ens.domains/	Open source decentralised naming protocol
Glassnode	https://defillama.com	Defi dashboard
Immunefi	https://immunefi.com/research/	Bug bounty and security services platform for Web3
Nyckel	https://www.nyckel.com/nft-finder	NFT finder (with text or image)
Openchain	https://openchain.xyz/trace	Transaction tracer (7 blockchains)
Rekt	https://de.fi/rekt-database	database of DeFi scams, hacks and exploits
Sentio	https://app.sentio.xyz/explorer	full-stack crypto data platform
C. Smart contracts		
Dedaub	https://dedaub.com/	Ethereum-compatible decompilation, formal methods and security monitoring platform
Ethereum Signature database	https://www.4byte.directory/	
EVM codes	https://www.evm.codes/	Opcode interactive reference
Oko	https://oko.palkeo.com/	Smart contract explorer
D. Crypto outreach – basic knowledge		
Ethereum.org	https://ethereum.org/	
Elemental crypto	https://elementalcrypto.com/tag/decentralized-finance/	'Crypto made Simple'
Finematics	https://finematics.com	Valuable outreach on DeFi

9. Glossary

Aggregator	DeFi aggregators bring together trades across various decentralised finance platforms into one place. They aim to optimise trades by pulling competitive prices from across the DeFi landscape. DeFi aggregators permit users to analyse and combine other users' trading strategies, which could potentially make the process more efficient and user-friendly.
Atomic swap	Atomic swaps enable peer-to-peer exchanges of crypto tokens across different blockchain networks that only execute if both parties each deposit a predetermined amount of tokens to the exchange contract. This enables any two users to swap digital tokens without relying on a third party to facilitate the transaction – thereby reducing counterparty risks.
Automated Market Makers (AMM)	Type of decentralised exchanges that use algorithmic mechanisms to facilitate the trading of digital assets. Unlike traditional financial markets that rely on buyers and sellers, AMMs aim to maintain liquidity in the DeFi ecosystem through liquidity pools. These pools are supplied with crypto tokens by users, and the prices of these tokens are determined by a constant mathematical formula.
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.
Bot	Also called a web robot or a robot, it is a software application that runs automated tasks (scripts) on the Internet, usually with the intent to imitate human activity, such as messaging, on a large scale.
Bridge	A protocol enabling the transfer of assets and data across different blockchain networks, either unidirectionally or bidirectionally, without relying on centralised intermediaries.
Bytecode	Bytecode is a low-level, machine-readable representation of code, executed by a virtual machine. Bytecode is a compact binary format consisting of opcodes (operation codes) and data. It acts as an intermediary between high-level source code and the virtual machine, enabling execution of programs.

Centralised exchange (CEX)	Digital platform operated by a central authority. It facilitates the trading, buying, and selling of various cryptocurrencies. Acting as an intermediary, CEXs connect buyers and sellers. They provide an online marketplace where users can exchange crypto-assets for other or fiat currencies. These exchanges typically offer custodial services. This means they hold users' funds in their wallets. It simplifies the trading process but requires users to trust the exchange's security measures.
Centralised decentralised finance (CeDeFi)	CeDeFi combines traditional centralised financial services with decentralised applications, merging conventional regulatory policies with modern financial products while meeting conventional financial regulatory standards.
Centralised finance (CeFi)	Centralised finance encompasses crypto-assets related financial services such as trading, lending, borrowing, and yield-earning opportunities that operate through centralised institutions rather than decentralised protocols. It represents an intermediate approach between traditional finance and decentralised finance, combining elements of both worlds.
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.
Collateral	Collateral represents any asset that is offered as security when someone takes out a loan. The idea behind collateral is to ensure that the borrower is going to either pay back the loan to get back the collateral or the lender will have the equivalent of the sum borrowed. The way collateral works depends on the agreement signed by the lender and the borrower.
Cold wallet	Also known as offline storage or cold storage, is a type of crypto-asset wallet that remains disconnected from the internet, giving users or institutions full control over their private keys. This separation from online networks makes cold wallets one of the most secure ways to store digital assets.
Crimeware-as-a-service (CaaS)	This involves experienced criminals selling their tools and services to less experienced offenders for a price. This model resembles software-as-a-service (SaaS), where the provider gives access to the software to the subscriber. In the case of crimeware-as-a-service, the SaaS model has reshaped itself in the context of cybercrime.

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 crypto-assets, non-fungible tokens, stablecoins, and security tokens.
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.
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.
Decentralised applications (dApps)	Applications that run on blockchain networks, striving to provide enhanced security, transparency, and autonomy. Decentralised applications are powered by smart contracts and operate on a peer-to-peer network, eliminating the need for a central authority. While dApps present several potential benefits, they face challenges such as scalability and potential security breaches.
Decentralised exchange (DEX)	Decentralised exchanges act as an alternative to centralised exchanges. They are non-custodial and allow users to operate anonymously. Crypto-assets trades are typically handled by the user and their crypto-asset wallet.
Decentralised finance (DeFi)	Decentralised finance is an emerging financial system using blockchain and crypto-assets to enable direct transactions between individuals and businesses. By eliminating intermediaries like banks, DeFi aims to reduce costs and speed up processes, although it's currently in its infancy and presents security challenges.
Decentralised organisation (DAOs)	DAOs are a revolutionary form of governance enabled by blockchain technology. Unlike traditional organisations, DAOs operate without a central authority, using smart contracts and community-driven decision-making to manage their operations.
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.
Drainer	This refers to a malicious tool designed to drain crypto-assets or traditional financial assets from a compromised account, wallet, or online platform. These tools target everything from crypto wallets to bank accounts and e-commerce platforms, allowing attackers to steal funds quickly and anonymously.
Draining-as-a-service (DaaS)	Threat actors and groups are offering the use of drainers as a service. This means that they are selling the tools for others to use. This allows others to purchase, on the dark web, drainers on demand. They will also often be accompanied by support for any issues as well as tutorials on how to use the tools.
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.
Ethereum Virtual Machine (EVM)	Decentralised computation engine that executes smart contracts on the Ethereum network. It is a crucial component of Ethereum's infrastructure, enabling the execution of code exactly as intended.
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.
Gas	Gas fees are transaction costs on the Ethereum blockchain, paid in Ether (ETH) or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.
Hacking	The unauthorised access to crypto wallets or exchanges, often with the intent to steal funds or exploit system vulnerabilities.
Hash	A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Regardless of the original amount of data or file size involved, its unique hash will always be the same size.

Initial Coin Offering (ICO)	An Initial Coin Offering is a fundraising mechanism in the crypto-asset industry, similar to an Initial Public Offering (IPO) in the traditional financial sector. Companies aiming to gather resources for the creation of a new coin, application, or service can launch an ICO. Participants interested in the project can acquire tokens during the ICO and receive a new crypto-asset token issued by the company. This token may have utility related to the product or service the company provides or represent a stake in the company or project.
Lending	Crypto lending is a financial transaction where one party lends crypto-assets to another party in exchange for compensation. This process is similar to traditional lending, but instead of banks, crypto lending is facilitated by crypto lending platforms.
Lightning network	The lightning network is a “second layer” payment protocol that operates on top of a blockchain. It is designed to enable fast, scalable transactions between and across participating nodes, and has been touted as a solution to Bitcoin’s scalability problem. Transactions are normally conducted on the blockchain, but Lightning involves taking transactions off-chain.
Liquidity pool	Liquidity pools are a mechanism by which users can pool their assets in a DEX’s smart contracts to provide asset liquidity for traders to swap between assets. Liquidity pools provide much-needed liquidity, speed, and convenience to the DeFi ecosystem.
Minting	Process of generating new coins by authenticating data, creating new blocks, and recording the information onto the blockchain through a “proof of stake” protocol. Both new units of a crypto-asset and NFTs can be minted this way.
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.
Multi signature (Multi Sig)	Security feature that necessitates multiple keys to authorise a crypto-asset transaction. Multi Sig wallets aim to provide improved protection, particularly for businesses or groups that need to safeguard their digital assets.
Nested service	Nested services, also known as “parasite exchanges” represent a form of financial intermediation that exploits the infrastructure of legitimate crypto-asset exchanges while circumventing regulatory requirements. These services function by opening accounts with regulated exchanges under various identities – often using shell companies or fraudulent credentials – and then providing their own customers with access to trading services through these accounts.

Node	A crypto node is a computer that is part of a blockchain network. Nodes validate and process transactions without the need for a centralised entity, striving to ensure the integrity and security of the network.
Non-Fungible Token (NFT)	A unique crypto-asset that is not interchangeable with another due to its distinct characteristics (e.g. digital art, collectibles, real estate, in-game elements or even precious metals). Unlike fungible assets, each NFT has individual value and properties and cannot be replicated nor replaced by another asset.
On-chain/ off-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.
On-ramp/ off-ramp	Fiat on-ramps and off-ramps are services that facilitate the exchange of fiat currencies for crypto-assets and vice versa. On-ramps and off-ramps play a role in the adoption of crypto-assets, providing a bridge between traditional finance and the digital asset marketplace.
Operation codes (Opcode)	Basic building blocks in Bitcoin Script that define and enable various operations on the network. They allow users to set transaction conditions, manipulate data on the stack, execute calculations, validate or invalidate transactions, and perform cryptographic functions, among other functions.
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.
Optimistic rollups	Optimistic rollups operate on an “optimistic” approach to executing off-chain transactions. This means they assume all Layer 2 transactions are valid unless challenged and proven wrong by an honest network validator. They use a “fraud-proof” mechanism to detect invalid transactions. If a fraud-proof is valid, it nullifies the faulty transaction and re-executes it to update the rollup’s state. However, if the optimistic rollup batch is unchallenged during the dispute period, the transaction data are successfully added to the Ethereum main chain.
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.

Peeling chain	Technique used to launder a large amount of crypto-assets through a lengthy series of minor transactions. A small portion is “peeled” from the subject’s address in a low-value transfer. These incremental outputs are often directed to exchanges where they can be converted to fiat currency (e.g. dollars) or other assets. The subject’s remaining assets passes to a new change address and the process repeats.
Peer-to-peer (P2P)	Peer-to-peer is a distributed networking or computing architecture that divides tasks or workloads across several computer systems (each one acting as an individual peer). P2P networks can be used to share any kind of digital data, including crypto-assets.
Peg	A “peg” is a specified price for the rate of exchange between two assets. This is in direct contrast to “floating” assets which have no hard price target and follow looser monetary policy.
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.
Private key	A private key is like a password – a string of letters and numbers – that allows users to access and manage their crypto funds. A private key gives the ability to prove ownership or spend the funds associated with the public address.
Proof-of-Stake (PoS)	Consensus mechanism that reduces the need for computational power by using randomly selected validators to confirm transactions and create new blocks, significantly lowering energy consumption compared to Proof-of-Work. Validators in a PoS system must stake a certain amount of crypto-assets as collateral to be selected for block validation, promoting network security and reducing environmental impact.

Proof-of-Work (PoW)	Proof of work is the original crypto consensus mechanism, first used by Bitcoin. Proof of work and mining are closely related ideas. The reason it's called "proof of work" is because the network requires a huge amount of processing power. Proof-of-work blockchains are secured and verified by virtual miners around the world racing to be the first to solve a math puzzle. The winner gets to update the blockchain with the latest verified transactions and is rewarded by the network with a predetermined amount of crypto.
Public key	A public key allows users to receive crypto-assets transactions. It is a cryptographic code that is paired to a private key. While anyone can send transactions to the public key, users need the private key to "unlock" them and prove that they are the owner of the crypto-assets received in the transaction.
Recovery phrase/seed	A series of words generated by the crypto-assets wallet that gives users access to the crypto associated with that wallet. As long as users have their recovery phrase, they will have access to all of the crypto associated with the wallet that generated the phrase — even if they delete or lose the wallet.
Regulatory sandbox	A regulatory sandbox is a controlled environment, established to understand the opportunities and risks associated with specific innovations and to develop an appropriate regulatory environment to accommodate them effectively.
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.
Scalability	Scalability refers to a blockchain network's ability to process more transactions per second without sacrificing network security.
Self-hosted wallet	A self-hosted wallet refers to a type of digital wallet that is hosted and controlled by the user, as opposed to being hosted by a third-party service, like a CASP.
Sidechain	Sidechains are independent blockchains that connect to their parent chains via a two-way bridge. This bridge allows the transfer of assets between the two.
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.
Total Value Locked (TVL)	Crypto-asset metric used to measure the total value of digital assets locked or staked on a particular decentralised finance platform or decentralised application.
Traditional finance (TradFi)	This refers to the conventional financial systems that have been in place for many decades. This framework encompasses a wide range of financial services provided by established institutions such as banks, insurance companies, stock exchanges, and other regulated entities.
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.
Validator	A validator is a participant in a blockchain network tasked with confirming transactions and adding them to the blockchain.
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.

Yielding	Leveraging strategies like lending, staking, or actively managed strategies to generate returns over time without actively trading.
Zero-Knowledge Proof	A cryptographic protocol enabling one party to prove the truth of a statement without revealing any underlying data. For example, verifying identity without disclosing personal details.
Zero-Knowledge (ZK) Rollups	ZK-Rollups are rollups where validators prove a transaction's authenticity without revealing any transaction details. Unlike optimistic rollups, ZK-Rollups assume all transactions are false until proven valid through Zero-Knowledge Proofs. They rely on "validity proofs" to determine if a transaction is true or not. ZK rollup nodes have to provide validity proofs for all transactions to ensure that the transaction data on the Ethereum chain is valid.

This study provides financial intelligence units and law enforcement authorities with a clear understanding of decentralised finance, its associated ML/TF risks, and the operational challenges it creates. It offers practical tools and resources for analysing and investigating DeFi-related financial flows, identifies key obstacles that may hinder effective action, and presents emerging typologies and risks. By outlining best practices and concrete recommendations – covering training, cooperation, and the use of specialised analytical tools – the study aims to strengthen the capacity of investigative and analytical services to address the rapidly evolving threats linked to this transformative financial ecosystem.

The Economic Crime and Cooperation Division (ECCD) at the Directorate General Human Rights and Rule of Law of the Council of Europe is responsible for designing and implementing technical assistance and co-operation programmes aimed at strengthening the capacities of Council of Europe member states and non-member states and jurisdictions to combat corruption, money laundering and terrorist financing, enhancing their asset recovery systems, and international cooperation.

www.coe.int

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.