Revista Científica del Centro Universitario de la Guardia Civil

Revista Logos Guardia Civil

Research Article

MONEY LAUNDERING THROUGH CRYPTO-ASSETS: REGULATORY EFFECTIVENESS AND THE GAP BETWEEN TECHNOLOGICAL TRACEABILITY AND LEGAL ATTRIBUTION IN THE EUROPEAN UNION AND THE UNITED STATES

English translation with AI assistance (DeepL)

Benjamín Garcinuño Roldán
PhD candidate at the UNED International Doctoral School (EIDUNED), member of Guardia Civil, practising lawyer at the Córdoba Bar Association. Master's degree in Security, Bachelor's degree in Law
bgarcinun2@alumno.uned.es
https://orcid.org/0009-0005-6923-1004

Received 25/02/2026
Accepted 02/06/2026
Published 30/06/2026

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913

Recommended citation: Garcinuño B. (2026). Money laundering through crypto-assets: regulatory effectiveness and the gap between technological traceability and legal attribution in the European Union and the United States. *Revista Logos Guardia Civil*, 4(2), pp. 215–252. https://doi.org/10.64217/logosguardiacivil.v4i2.8913

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
Online ISSN: 2952-394X

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

DEDICATION

To Mariam, for trusting me,
and for feeding the birds in my head.
I must remind her that the sun is still shining, even if she doesn't look at it.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

MONEY LAUNDERING THROUGH CRYPTO-ASSETS: REGULATORY EFFECTIVENESS AND THE GAP BETWEEN TECHNOLOGICAL TRACEABILITY AND LEGAL ATTRIBUTION IN THE EUROPEAN UNION AND THE UNITED STATES

Abstract: Money laundering is a dynamic phenomenon whose evolution is linked to the international economic environment. Methods of laundering illicit funds pose new regulatory and operational challenges to authorities and financial institutions, driven largely by technological developments. Through the use of certain recent technologies, they create an environment of pseudonymity, which transcends its purely technical nature. This feature acts as a strategic tool for criminal organisations (COs) seeking to refine their money-laundering schemes, enabling them to conceal the traceability of funds and the consequences of the underlying harm**.** This article critically analyses the issue of illicit funds being laundered via crypto-assets by COs and the various strategies employed by COs to conceal their traceability and identity. Firstly, international instruments such as the United Nations Convention against Transnational Organised Crime and the recommendations of the Financial Action Task Force (FATF) are systematically examined in relation to the system for prosecuting and preventing the laundering of illicit funds through crypto-assets. Building on this international framework, this paper is

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

structured around a comparative analysis of the legislative frameworks—which differ substantially—regarding money laundering through crypto-assets in the United States (US) and the European Union (EU). This study is not limited to a descriptive analysis of the phenomenon, but rather highlights the need to strengthen the regulatory framework by identifying significant legislative divergences, legal loopholes and limitations in supervisory mechanisms.

Resumen: El blanqueo de capitales es un fenómeno dinámico cuya evolución está vinculada al entorno económico internacional. Los métodos de blanqueo de capitales ilícitos generan nuevos desafíos regulatorios y operativos a las autoridades y a las entidades financieras, en gran medida impulsados por el desarrollo de la tecnología. Con el uso de ciertas tecnologías recientes, generan un entorno de seudonimidad, el cual trasciende su naturaleza meramente técnica. Este rasgo opera como un instrumento estratégico para las organizaciones y grupos criminales (OC) que buscan sofisticar sus esquemas de blanqueo, permitiendo la ocultación de la trazabilidad y la consecuencia de los daños subyacentes**.** El presente artículo analiza críticamente la problemática del blanqueo de fondos ilícitos mediante criptoactivos por parte de las OC y las diversas estrategias que emplean los OC para ocultar su trazabilidad e identidad. En primer lugar, se examinan de manera sistemática los instrumentos internacionales como son la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y las recomendaciones del Grupo de Acción Financiera Internacional (GAFI) en relación con el sistema de persecución y prevención del blanqueo de fondos ilícitos mediante criptoactivos. A partir de este marco internacional, el presente trabajo se articula en torno a un análisis comparativo del marco legislativo, sustancialmente diferentes frente al blanqueo de capitales mediante criptoactivos en los Estados Unidos (EE. UU) y la Unión Europea (UE). El presente estudio no se limita a una aproximación descriptiva del fenómeno, sino que pone la necesidad revisión de reforzar la arquitectura regulatoria, mediante la identificación de divergencias legislativas significativas, lagunas jurídicas y limitaciones en los mecanismos de supervisión.

Keywords: Crypto-assets, money laundering, organised crime, digital pseudonymity, financial regulation, emerging technologies, the darknet, transparency and beneficial ownership.

Palabras clave: Criptoactivos, blanqueo de capitales, criminalidad organizada, seudonimidad digital, regulación financiera, tecnologías emergentes, darknet, transparencia y titularidad real.

ABBREVIATIONS

AML: *Anti-Money Laundering*. In Spanish: the fight against money laundering.

AMLA: *Anti-Money Laundering Authority*. In Spanish: European Authority for Combating Money Laundering and Terrorist Financing.

AMLC: *Anti-Money Laundering Council*. In Spanish: Council against money laundering.

BARIS: *Bank Account Registers Interconnection System.* In Spanish: European Union Bank Account Registers Interconnection System.

BC: Money laundering.

BSA: *Bank Secrecy Act.* In Spanish: Ley de Secreto Bancario.

CDD: *Customer Due Diligence*. In Spanish: Diligencia Debida en relación con el Cliente (DDC).

CEO: *Chief Executive Officer*. In Spanish: director ejecutivo or Consejero Delegado, depending on the country.

CFT: *Countering the Financing of Terrorism.* In Spanish: Lucha contra la Financiación del Terrorismo.

CFTC: *Commodity Futures Trading Commission.* In Spanish: the independent US federal agency that regulates derivatives markets (futures, *swaps* and certain options).

DAO: *Decentralised Autonomous Organisation*. In Spanish: in the context of anti-money laundering (AML/CFT), this is a *blockchain-native* organisation that coordinates decisions and manages assets through *smart contracts* and token-based governance, without a traditional central management structure.

DEA: *Drug Enforcement Administration*. In Spanish: Administración para el Control de Drogas.

US: United States.

EUR: Euro.

FATF: *Financial Action Task Force*. In Spanish: GAFI.

FBI: *Federal Bureau of Investigation*. In Spanish: the US Federal Bureau of Investigation and its main federal law enforcement agency.

FinCEN: *Financial Crimes Enforcement Network.* In Spanish, this is usually translated as 'Red de Control/Ejecución de Delitos Financieros'.

FT: Terrorist financing.

GAFI: Financial Action Task Force.

AI: Artificial intelligence.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

IEEPA: *International Emergency Economic Powers Act*. In Spanish: Ley de Poderes Económicos en Emergencias Internacionales.

ICO: *Initial Coin Offering*. In Spanish: Oferta Inicial de Monedas.

IRS: *Internal Revenue Service*. In Spanish: the US Federal Tax Collection Agency.

KYC: *Know Your Customer*. In Spanish: Conoce a Tu Cliente.

MiCA: *Markets in Crypto-Assets*. In Spanish: Regulation on Markets in Crypto-Assets.

NCA: *National Crime Agency*. In Spanish: UK National Crime Agency.

NYDFS: *New York State Department of Financial Services*. In Spanish: Departamento de Servicios Financieros del Estado de Nueva York.

OC: Criminal organisation.

PBC/FT: Prevention of money laundering and terrorist financing.

SEC: *Securities and Exchange Commission*. In Spanish: US Securities and Exchange Commission.

SEPBLAC: Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences.

STR: *Suspicious Transaction Report*. In Spanish: Reporte de Transacción Sospechosa.

UIF: Financial Intelligence Unit. In Spain, this is SEPBLAC (Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences).

UNODC: *United Nations Office on Drugs and Crime*. In Spanish: Oficina de las Naciones Unidas contra la Droga y el Delito.

UNTOC: *United Nations Convention against Transnational Organised Crime*. In Spanish: Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

USD: *United States Dollar*.

VASP: *Virtual Asset Service Provider*. In Spanish: Proveedores de Servicios de Activos Virtuales or CASP within the European framework.

6AMLD: Sixth Anti-Money Laundering and Counter-Terrorist Financing Directive.

1. INTRODUCTION

In recent years, crypto-assets have revolutionised the world of finance, opening the door to innovation and financial inclusion on an unprecedented scale. However, this technological progress has also given rise to new challenges, particularly in the field of financial crime. One of the most worrying issues is the use of crypto-assets for money laundering (ML) by criminal organisations or groups (COs).

These assets generally operate on decentralised networks known as *blockchains,* which ensure transparent and secure transactions without the need for a centralised third party such as a bank (Bhutta et al., 2021). When a cryptocurrency is transferred, the transaction is recorded on *the blockchain*, which functions as a public ledger distributed across many computers worldwide (Soltani et al., 2022). Transactions are verified by a network of users known as miners, who are rewarded with new units of crypto-assets (Binance Academy, 2024).

For decades, money laundering (ML) has been a global problem. Concealing the source of illegally obtained funds has been the primary objective of organised crime (OC) groups, with the firm aim of giving these funds a legal appearance within economic systems. Using this technique, OC groups were able to invest their illegal profits without leaving a financial trail that could lead to their discovery and prosecution.

Conventional organised crime groups are highly structured, with defined hierarchies and roles for their members (Enríquez Pérez, 2020); they are often supported by local politicians and use corruption to avoid problems with the police (Luna Galván et al., 2021). They operate through decentralised structures that make it difficult to identify their activities (UNODC, 2024). The structure of such OCs is designed to protect them from law enforcement and reduce the risk of infiltration or betrayal (UNODC.1, 2024). To ensure a common definition of organised crime amongst Member States, the United Nations Convention against Transnational Organised Crime was established. This Convention defines an OC as a structured group of three or more persons acting in concert to commit offences with the aim of obtaining a direct or indirect financial benefit (Akkoyun & Çelik, 2022).

OCs, with a high level of specialisation in the use of complex financial tools, are increasingly using virtual currencies to conceal the origin of their illicit funds (Trozze et al., 2022). OCs employ techniques such as layering[1] , mixing services and cross-border transfers to make it difficult to trace funds. (Arnone et al., 2025). The incorporation of *blockchain* analysis tools and the strengthening of KYC/AML/CFT (Anti-Money Laundering and Counter-Terrorist Financing) obligations make it possible to optimise the detection and control of illicit transactions. (Rodríguez-Valencia et al., 2025).

The following article addresses the issue of money laundering involving illicit funds via crypto-assets by organised crime groups (OCGs) and the existing legal framework to combat it. The analysis includes the FATF's recommendations, international instruments and the regulations of the United States (US) and the European Union (EU) aimed at

[1] *Layering* is the second stage of the money laundering process, in which the main objective is to conceal the illicit origin of the funds through a series of complex, successive and often cross-border financial transactions. This stage aims to break the traceability of the money and make it difficult for the authorities to reconstruct the original path of the funds.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

preventing money laundering via crypto-assets by organised crime groups. This paper examines the international treaties and national laws of the US and Europe that seek to prevent money laundering by organised crime groups.

Building on this premise, this article presents a comparative analysis of the regulatory models in the US and the EU, with the aim of identifying their strengths and weaknesses and formulating legal assessment criteria. Furthermore, this paper argues that institutional efforts to mitigate money laundering via crypto-assets are effective only if they do not rely solely on the formal development of regulatory frameworks. Moreover, their degree of effectiveness depends on the actual capacity to prevent, detect, attribute and sanction unlawful conduct in an environment characterised by pseudonymity, technological decentralisation and the transnational dimension of the phenomenon.

The main contribution of this study lies in identifying the existence of a structural gap between the technical traceability of *blockchain* transactions and their effective legal attribution. Consequently, conventional models of prevention, detection and sanctioning—which incorporate technological capabilities into regulatory systems—must be re-examined.

2. RESEARCH METHODOLOGY

This document adopts a descriptive analytical approach. The analysis will be multidimensional, examining legislation, the literature and relevant information to assess the measures taken by financial institutions to prevent the laundering of crypto-assets. An exploratory review of the existing literature (books, journals, articles, etc.) will provide a better understanding of the concept, the nature of the issue and the most effective ways of addressing it.

This approach constitutes the most appropriate methodology for conducting the research, given the lack of information and the scarcity of articles discussing the FATF recommendations, international conventions and national legislation in the US and Europe regarding the issue of crypto-asset money laundering by COs.

Furthermore, the study incorporates a proactive analytical dimension, aimed at identifying the structural limitations of the current legal framework in decentralised digital environments.

3. ANALYSIS OF THE (MIS)USE OF CRYPTO-ASSETS BY CRIMINAL ORGANISATIONS

The proliferation of clandestine banking services and other online money-laundering networks has created more anonymous channels for financial transfers (Europol, 2022). Crypto-assets have the potential to be misused by criminals; as a result , the industry is developing new, complex forms of peer-to-peer mixing services. This creates the conditions for concealing transactions, decentralised *blockchain* analysis, and the new peer-to-peer networks that have recently emerged and are likely to be used for illegal activities (Hinojal, 2023). Such developments will significantly hinder the identification of criminal organisation activities that use conventional cryptocurrencies to conceal illicit proceeds (Fu et al., 2025).

Drug trafficking, arms trafficking and the trafficking of other illegal goods are lucrative ventures, insofar as illicit funds can be easily moved to and from organised crime groups anywhere in the world (Sudan et al., 2023). Indeed, beyond scams, crypto-assets have been linked to almost every type of cybercrime, ranging from services on the *deep web*[2] or *darknet*[3] to theft and fraud in their many forms.

Crypto-assets have been used in a variety of organised crime (OC) activities, including money laundering, *ransomware* attacks[4] and online fraud. In order to combat these illicit practices, law enforcement agencies have been provided with an overview of the existing literature on the subject (Trozze et al., 2022). Research into misuse by organised crime remains limited compared to other areas of research on crypto-assets and *blockchain*. Among the illegal activities carried out by organised crime using digital currencies are money laundering (proceeds of crime), *ransomware* and black markets (Alessi Longa, 2025).

Seven categories have been identified, each of which encapsulates a specific pattern of criminal behaviour in the use of crypto-assets and its implications for prevention, detection and response mechanisms:

(1) the financing of terrorism, (2) on the dark web, (3) on *deep web* or *darknet* markets, (4) in cybercrime, (5) in drug trafficking, (6) in human trafficking, (7) and in corruption.

We will focus our research on option 2:

4. CRYPTO-ASSETS AND MONEY LAUNDERING BY CRIMINAL ORGANISATIONS

Crypto-assets received by illicit addresses in 2023 amounted to 46,100 million US dollars (Chainalysis, 2025). In 2024, the value received by illicit addresses plummeted to US$40,900 million. However, the figures for 2024 are provisional and could easily exceed US$51,000 million (Atlam et al., 2024).

Whilst some argue that crypto-assets entail high information and control costs, transactions are generally cheaper and faster than those involving fiat currencies, as there are no intermediaries between buyers and sellers (Medranda Morales & Arcos Argudo, 2023). Yet these very characteristics have been exploited by organised crime groups for money laundering. In particular, three characteristics of crypto-assets drastically reduce the transaction costs of these illegal activities.

Firstly, the decentralised nature of crypto-assets enables users to exchange value directly with one another without the need for intermediaries. As already mentioned,

[2] The deep web is the part of the internet that is not indexed by conventional search engines, such as Google, Bing or Yahoo. This means that its content cannot be found through normal searches and is only accessible if the address is known directly, if authorisation is granted, or if specific credentials are used.

[3] The darknet is a specific and deliberately hidden part of the internet that can only be accessed via special software, configurations or protocols that provide anonymity, such as Tor, I2P or Freenet. It is not indexed by conventional search engines and is designed to protect the identity and location of users and servers.

[4] *Ransomware* is a type of malicious software (*malware*) designed to lock, encrypt or render a victim's computer systems inoperable, with the aim of demanding a financial ransom — usually in cryptocurrencies — in exchange for restoring access to data or systems.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

traditional anti-money laundering regulations are designed to regulate intermediaries carrying out transactions in order to prevent illegal transfers (Longa, 2025), and the absence of face-to-face interactions in crypto-asset transactions makes it more difficult to identify the parties involved (Montoya Arrubla, 2025). Secondly, whilst all transactions are recorded and traceable on the *blockchain*, there is no explicit link to the actual individuals or organisations behind them. Crypto-assets operate within a pseudonymous system in which only the public key (a random string of numbers) is known, whilst the private key remains secret.

This makes it significantly more difficult to link a real identity to a cryptocurrency address (Béres et al., 2021). However, users can generate multiple electronic crypto-asset wallets with different public addresses, which hinders traceability in cases of suspected money laundering (Atlam et al., 2024).

Finally, the speed of crypto-asset transactions and their ease of use give them an advantage over traditional money-laundering methods, such as cash. Unlike paper money, which is limited by weight and size, crypto-assets can be stored in unlimited quantities on a USB stick and sent to anyone in the world in a matter of minutes. The malleability of transactions makes it easier to circumvent regulatory measures, as a large transaction can be split into smaller ones (Koelbing et al., 2024). This operational flexibility is vital and reinforces money laundering for organised crime groups operating in crypto-asset markets. Such groups generate a large volume of crypto-assets, which they need to convert into funds with a legitimate appearance.

This process generally involves a series of complex financial transactions that move funds through multiple accounts and jurisdictions, making it difficult to trace the origin of the funds. This enables COs to continue operating illegally and conceal the proceeds of drug trafficking (FATF, 2022). Criminal organisations that use the *deep web* are experts in laundering crypto-assets, which can be transferred instantly from one account to another and are difficult to trace (Holt et al., 2023). Such criminal organisations often hire professional facilitators (lawyers, accountants, bankers, etc.) to make it harder to trace their illicit funds.

Criminal organisations may hold on to the crypto-assets they receive from crypto-market transactions as an investment. These are used to launder other illicit funds both online and in the real world (Arnone et al., 2025). Those not retained as an investment are laundered and channelled into the legitimate economy. For example, the Dutch police discovered that a moderator of a crypto marketplace was exploiting his contacts to exchange bitcoins for cash (Ministry of the Interior, 2024).

In East and South-East Asia, '*point* runners' or '*moving* ants' organisations are used to launder illicit funds, recruiting large numbers of people (often unemployed young people) who lend their bank accounts and set up shell companies to conceal the source and destination of the illicit funds (UNODC, 2025). These networks move the funds through multiple bank or crypto-asset accounts and online casinos, where they are disguised as legitimate casino winnings (Langdale, 2024).

Now that the authorities have a better understanding of third-party payments (following '*Operation Chain* Break' and similar operations in China) (FinCEN, 2025),

organised crime groups have increasingly turned to crypto-assets for their illegal gambling operations, posing serious challenges for investigators (Europol, 2024). For example, casinos and *junket* operators[5] licensed in the Philippines were involved in laundering some US$81 million stolen in a 2016 cyberattack attributed to the Lazarus Group from the Central Bank of Bangladesh (Langdale, 2024). Although the funds passed through banks and remittance companies, it was extremely difficult to trace them once they reached the casino junket operators (AMLC, 2023).

Global drug cartels were accused by the DEA of using *Binance*,[6] – the largest cryptocurrency exchange – to launder between 15 and 40 million dollars in various transactions (DEA, 2025). According to DEA reports, *Binance* is cooperating with investigators amid scrutiny over various allegations.

These sophisticated mechanisms pose new challenges for detection and investigation due to the volume of transactions and their cross-border nature, requiring greater financial transparency, international cooperation and stronger regulatory frameworks to combat such crimes (Legrand & Leuprecht, 2021).

5. MOST COMMON METHODS OF CRYPTO-ASSET MONEY LAUNDERING USED BY CRIMINAL ORGANISATIONS

5.1. GENERAL CONSIDERATIONS FROM THE PERSPECTIVE OF MONEY LAUNDERING THEORY

The phenomenon under consideration highlights that the various techniques employed by organised crime groups fall within the classic phases of money laundering, in particular placement, layering and integration.

These practices, described in the previous section, are what give rise to problems regarding criminal classification, the attribution of liability and the reconstruction of the financial trail of illicit funds. This is particularly true in an environment characterised by pseudonymity and technological decentralisation, such as that of crypto-assets.

5.2. TECHNIQUES RELATED TO THE INTEGRATION PHASE: *SMURFING*

The practice known as *smurfing*, or ‘breaking up large sums into small ones’, involves integrating funds obtained through illicit activities—such as proceeds from drug trafficking, payments from fraud, corruption or profits derived from sexual exploitation—into the financial system in a varied manner and in small amounts (Isolauri & Ameer, 2023). This technique, used in conventional finance, appears to have been transferred to the world of crypto-assets (Koelbing et al., 2024).

[5] Junket operators are specialised intermediaries who act as a link between casinos and VIP or high-roller players, particularly in markets such as Macau, Las Vegas, Singapore and other international gambling hubs. Their main role is to recruit, transport, finance and manage high-value clients so that they gamble at specific casinos.

[6] Binance is the world’s largest cryptocurrency exchange by trading volume and number of users, founded in 2017 by Changpeng Zhao (CZ) and Yi He. It is a centralised exchange (CEX) that allows users to buy, sell, trade and hold digital assets.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

From a criminal law perspective, such practices may fall within the integration phase of money laundering. It is clear that the intention is to introduce illicit funds into the official financial system by splitting them up, in order to circumvent control mechanisms. From a legal perspective, this raises significant questions regarding the application of regulatory thresholds and the effectiveness of automated detection systems.

5.3. TECHNIQUES RELATED TO THE STRATIFICATION PHASE: CONCEALMENT AND DISASSOCIATION OF ILLICIT ORIGIN

5.3.1. Crypto-asset wallets (medium wallets or mid-size wallets)

A common money laundering method involving crypto-assets entails the use of intermediary wallets. This layering technique seeks to conceal the link between illicit funds and their subsequent entry into the legal financial system (Elliptic, 2024). Consequently, intermediary wallets are being used by criminals on both KYC-compliant and non-KYC-compliant *exchanges*.

From a theoretical perspective, intermediary accounts and their use are directly linked to the layering phase of money laundering, as they are intended to hinder the traceability of illicit funds. These described practices pose significant challenges regarding the objective attribution and identification of the beneficial owner, particularly when there are no points of contact with intermediaries obliged to carry out identification checks.

5.3.2. Consolidation crypto-asset wallets

Consolidation wallets, which pool and combine funds from various sources, are another trend to bear in mind. This consolidation pattern may reveal attempts to conceal the illicit origin of funds before moving them to exchanges or other locations for cash withdrawal (Chiang, 2024).

From a legal perspective, these structures could be regarded as instruments designed to reinforce the concealment of the illicit origin of the funds. This circumstance directly affects the typical configuration of the offence of money laundering in its form of concealment or cover-up.

5.3.3. Mixing services, privacy coins and bridges

The aim of mixing and shuffling is to break up large amounts of virtual currency by distributing them in multiple directions (Gorjón, 2023). Mixers are individuals or companies that distribute the funds amongst participants and mix them with legitimate income in order to obscure the traceability and identification of the owners (Coinmetro Editorial Team, 2024).

The specific issues regarding criminal liability in the concealment phase of money laundering arising from the use of mixing services are designed precisely to hinder the traceability of funds. Consequently, this issue calls into question the scope of the due diligence obligations of virtual asset service providers (VASPs) or CASPs within the European framework. This circumstance is addressed in Article 13 of Directive (EU)

2015/849, particularly where such providers operate in jurisdictions with limited or non-existent supervision.

Privacy coins exacerbate the problems associated with attributing transactions by reinforcing pseudonymity in terms of identity. This creates a significant operational limitation on the admissibility of evidence in criminal proceedings, particularly with regard to linking addresses to specific natural or legal persons. Privacy coins have become popular amongst those who wish to remain anonymous. (Cremers et al., 2024).

The transfer of assets between different *blockchains* is a technique known as crypto bridges, which is an increasingly popular method or tool for cross-border crime.

From a legal perspective, the use of *cross-blockchain* bridges exacerbates the transnational dimension of cybercrime, giving rise to issues of jurisdictional competition and international cooperation, as well as additional operational constraints in reconstructing the financial trail of funds.

5.4. CRIMINOGENIC SPACES AND FACILITATORS: *DARKNET* MARKETPLACES

Darknet markets are hidden online sites accessed via specific software (such as Tor) and paid for using anonymous crypto-assets. These markets facilitate the trade in illegal goods and services and provide money launderers with a means of converting illicit funds into crypto-assets and vice versa (Jordá et al., 2024). It is extremely difficult to determine precisely how much illicit money is laundered using this virtual asset (Alessi Longa, 2025).

On the darknet, *Silk Road* was the most popular marketplace operating on the *Tor* network, as it enabled anonymous trading using crypto-assets. Despite attempts to maintain pseudonymity, its founder, Ulbricht, was arrested by the FBI in 2013 and ultimately convicted on several charges.

Given the large volume of money laundering, it is pertinent to examine the existing legal framework with a view to combating the laundering of crypto-assets by organised crime groups. Such environments exacerbate the structural challenges faced by the authorities in intervening and pose regulatory and operational challenges both in obtaining digital evidence and in identifying the parties involved, which directly affects the effectiveness of criminal prosecution by the BC. The case illustrated the challenges of regulating and monitoring the *deep web* (Hemdani, 2025).

5.5. FINAL DOGMATIC CONSIDERATION

All these techniques highlight the limitations of conventional criminal law in adapting to decentralised technological structures. This raises questions about the definition of criminal offences and the effectiveness of regulatory responses in a constantly evolving digital environment.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

6. LEGAL FRAMEWORKS FOR COMBATING CRYPTO-ASSET MONEY LAUNDERING BY FINANCIAL CRIMINAL ORGANISATIONS

Legal frameworks for crypto-assets are highly fragmented globally, with some countries banning them outright and others embracing them fully. Attempts have been made through the United Nations Convention against Transnational Organised Crime (UNTOC) to combat transnational organised crime.

6.1. UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANISED CRIME

The UNTOC Convention of 2000 is the principal international legal instrument for addressing the challenges posed by transnational organised crime. It provides a set of tools for States to develop policies and legal frameworks to prevent and combat various forms of organised crime, such as money laundering associated with crypto-assets (Kabra & Gori, 2025). This convention is relevant insofar as such virtual assets are playing an increasingly significant role in the financial world of organised crime groups. The UNTOC can support the prosecution and prevention of crypto-asset money laundering through the development of stronger legal frameworks, international cooperation and the application of common standards to combat illegal transactions involving these virtual assets (Wang & Hsieh, 2023).

Articles 1, 13, 16 and 18 regulate cross-border cooperation on mutual legal assistance, extradition and the exchange of information. As transactions involving crypto-assets may span multiple jurisdictions, the UNTOC's focus on international cooperation is essential for identifying and bringing to justice organised crime groups that abuse these virtual assets. For example, the UK's National Crime Agency (NCA) dismantled a massive, multi-billion-dollar cryptocurrency network known as Operation Destabilise (Anggriawan & Susila, 2024).

This network served a wide range of organised crime groups, from wealthy Russians and global influencers to cybercriminals and drug traffickers. The NCA identified two Russian-speaking OC, 'Smart' and 'TGR', as the masterminds. To date, its investigation has led to 84 arrests and the seizure of over 20 million euros in cash and crypto-assets (UNODC2, 2024). This successful operation was made possible by the joint efforts of the signatories to the convention, including the , the UK Metropolitan Police Service, France's *Direction Centrale de la Police Judiciaire*, the US Treasury's Office of Foreign Assets Control, the Drug Enforcement Administration and the FBI. (FATF et al., 2025).

Article 34 of the UNTOC encourages States to adopt compatible legislative measures to prevent money laundering, which is essential for addressing the growing risks of financial crimes related to crypto-assets. For example, the FATF requires KYC and customer due diligence measures to identify and report suspicious crypto-asset transactions, which must be implemented in all countries, regardless of their local laws. (FATF, 2024).

The UNTOC supports the development of international standards, assisting countries in building enhanced cybersecurity and investigative capabilities to detect

crimes related to crypto-assets. UNODC. (2026) For example, the UNTOC's information-sharing channels support EU law enforcement agencies, such as Europol, in tracing illegal transactions involving this virtual asset. This may involve Eurojust, the EU agency for judicial cooperation, to ensure effective cross-border prosecution.

In this context, the UNTOC provides an international framework aimed at combating the laundering of crypto-assets by promoting international cooperation, legal harmonisation and capacity-building in the area of regulatory enforcement.

6.2. RECOMMENDATIONS OF THE FINANCIAL ACTION TASK FORCE

The FATF has established a comprehensive set of standards aimed at mitigating and combating ML/TF, covering virtual assets and virtual asset service providers (VASPs). From a legal perspective, the FATF defines 'virtual assets' and 'virtual asset service providers' to ensure the consistent and uniform application of its standards. Virtual assets are a digital representation of value that can be traded or transferred digitally and used to make payments or investments (FATF, 2023).

VASPs include any natural or legal person not otherwise covered by the Recommendations who, as a business, engages in one or more of the following activities: the exchange of virtual assets for fiat currencies; the exchange of virtual assets for one or more other forms of virtual assets; the transfer of virtual assets; the custody and/or management of virtual assets or instruments enabling the regulation of virtual assets; and the participation in and provision of financial services relating to the offering and/or sale of a virtual asset by an issuer (FATF, 2021).

From a legal perspective, Recommendation 15 deals specifically with virtual assets, stipulating that countries must identify and mitigate ML/TF risks associated with virtual assets and VASPs. The FATF requires the implementation of customer due diligence (CDD), record-keeping, the reporting of suspicious transactions (STR), internal controls and compliance programmes, and sanctions (FATF.1, 2023). Similarly, Recommendation 16 requires VASPs to obtain, retain and transmit information on the payer and payee for transfers of virtual assets above a specified threshold (1,000 USD/EUR). This is sometimes referred to as the 'travel rule'.[7]

This rule aims to prevent the use of virtual assets for illegal purposes and to ensure transparency in transactions, insofar as it requires VASPs to share this information with other obliged entities. The 'travel rule' for virtual assets has been a priority for the FATF, which continues to press countries to implement and enforce it (Mollaahmetoğlu & Baykut, 2021).

The FATF regularly updates its recommendations on virtual assets to keep pace with evolving risks and technological innovations in the world of virtual assets. Countries should incorporate these rules into their national laws and regulations. The FATF

[7] The Travel Rule is a requirement established by the Financial Action Task Force (FATF) which obliges financial institutions and virtual asset service providers (VASPs) to transmit information on the originator and the beneficiary alongside the transfer of funds or crypto-assets. Its purpose is to ensure traceability and enable the authorities to identify the parties involved in transactions that may be linked to money laundering, terrorist financing or other serious crimes.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

continues to monitor the implementation of these standards worldwide and urges jurisdictions to prioritise their effective implementation (Teng et al., 2026).

7. TRANSATLANTIC REGULATORY MODELS FOR COMBATING MONEY LAUNDERING INVOLVING CRYPTO-ASSETS: A COMPARATIVE ASSESSMENT OF THE US AND THE EU

7.1. UNITED STATES

In the US, there is no unified regulatory framework for crypto-assets; instead, various federal and state agencies oversee these virtual assets. The US *Securities and Exchange Commission* (SEC) regulates securities and has classified many crypto-assets and initial coin offerings (ICOs) as securities. In SEC v. *Decentralised Autonomous Organisation* (DAO), the SEC held that crypto-assets are securities and are therefore subject to SEC regulation (Lom & Hashmall, 2021). The *Commodity Futures Trading Commission* (CFTC), the US federal agency that regulates derivatives markets, considers Bitcoin and other virtual assets to be commodities and regulates derivatives and futures markets involving crypto-assets (Hinojal, 2023).

The *Financial Crimes Enforcement Network* (FinCEN) regulates crypto exchanges and e-wallet providers as money transmitters, and they must comply with AML/CFT and KYC regulations. The *Internal Revenue* Service (IRS) treats crypto-assets as property for tax purposes, and gains and losses are subject to capital gains tax (Baer et al., 2023). Regulation tends to be decentralised; states such as New York have their own laws (*BitLicense*),[8] whilst others have more lax or undefined policies.

The *BitLicense* is a business licence that requires operators to comply with stricter AML/CFT rules. In California, the law requires bitcoin operators to hold reserves equivalent to those of banks to cover losses, but North Carolina is still working on draft legislation to regulate bitcoin and has no regulations currently in force (NYDFS, 2024–2026).

The US Department of Justice brought criminal charges against *Rule and Nysewander*[9] for conspiring with others to launder illicit proceeds from online romance scams, business email compromise scams, property scams and other frauds via crypto-assets (Lim & Choi, 2025).

According to the indictment filed by the US Department of Justice, they had converted the illicit funds into crypto-assets and transferred them to accounts controlled by their accomplices in the US and abroad. This demonstrates a strategy designed to conceal the illicit origin of the funds and make them difficult to trace. Furthermore, when opening accounts and conducting transactions with banks and cryptocurrency exchanges, *Rule and Nysewander* are alleged to have made false statements and withheld relevant

[8] The *BitLicence* is a mandatory regulatory licence issued by the New York State Department of Financial Services (NYDFS) for companies conducting business involving cryptocurrencies or virtual assets in the state of New York or with New York residents. It was introduced in 2015 through Regulation 23 NYCRR Part 200.

[9] Two men (from Nevada and South Carolina) were charged and subsequently convicted of participating in a cryptocurrency money-laundering conspiracy, according to the US Department of Justice.

information in order to circumvent the controls and safeguards in place at these institutions.

As a result of these actions, in this alleged conspiracy, they and their accomplices laundered more than 2.4 million US dollars. Ultimately, both were found guilty and could face up to 20 years' federal imprisonment for each money laundering charge (Farrukh et al., 2025).

Similarly, in August 2024, Lam and Serrano were charged with the theft of crypto-assets worth US$230 million (Trozze et al., 2022).

US prosecutors have also targeted *Binance*, the company that operates the world's largest crypto-asset exchange platform, *Binance.com*. The company has pleaded guilty and will pay over US$4,000 million to settle the Department of Justice's investigation into breaches of the Bank Secrecy Act (BSA), for failing to register as a money transmitter, and of the International Emergency Economic Powers Act (IEEPA) (U.S. Department of Justice, 2023).

Changpeng Zhao, a Canadian national and founder and former CEO of *Binance*, also pleaded guilty to failing to maintain an effective anti-money laundering (AML) programme, in breach of the BSA. As part of the plea agreement, Zhao has resigned as CEO of Binance (U.S. Department of Justice.1, 2023).

Whilst US prosecutors have succeeded in prosecuting money launderers and cryptocurrency exchange platforms, the crypto-asset market still requires greater levels of transparency in order to protect potential investors (Anguren et al., 2023). A few decades ago, the boom in e-commerce led to innovative legal frameworks; today, these virtual assets and their many forms deserve similar guidance. The creation of clear rules for the sale of certain cryptocurrencies and crypto funds could provide much-needed clarity (Blanco Barón, 2025).

Without a more mature regulatory framework, relying solely on enforcement actions by agencies such as the SEC is insufficient to achieve its regulatory objectives. Ultimately, these punitive measures may harm the very investors the SEC seeks to protect and stifle investment in promising companies. Among the proposed regulations for crypto-assets is the draft bill against digital asset money laundering, which seeks to prevent other crimes related to virtual assets, whilst focusing on those carrying out the transactions (miners, validators, etc.) (Warren & Marshall, 2022).

From a legal perspective, the US system is characterised by being fragmented and reactive, as multiple agencies with interrelated powers are involved. The regulatory flexibility afforded by this structure can give rise to issues of regulatory consistency and potential overlaps in jurisdiction.

This approach has limitations in terms of *ex ante* prevention when it comes to BC, insofar as its actions are primarily centred on *enforcement* mechanisms that come into play after an offence has been committed. The regulatory shortfall of a unified framework likewise prevents the uniform application of compliance obligations by virtual asset service providers (VASPs); in this context, it could create areas of regulatory risk.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

7.2. EUROPEAN UNION

At present, the EU does not have a harmonised legal framework for crypto-assets across all Member States. However, the European Commission has proposed certain measures, such as the Sixth Anti-Money Laundering Directive (6AMLD), which would require firms dealing in crypto-assets to register with national authorities.

They would also be required to comply with anti-money laundering rules and report any suspicious transactions. The aim of 6AMLD is to close the legal loopholes in the individual laws of EU countries by establishing consistent definitions for cryptocurrency and virtual assets across the EU (European Parliament, 2024).

To establish a uniform approach to regulating trading in crypto-assets across the EU, the European Commission proposed the Regulation of the European Parliament and of the Council on Markets in Crypto-Assets and the amending Directive. This set of rules, known as MiCA ([10]), aims to establish a supervisory framework, including rules for issuers, service providers and participants in the secondary market.

Using these MiCA and 6AMLD regulations, on 19 September 2024, the German Federal Criminal Police dismantled the infrastructure of 47 Russian-language crypto-exchange platforms operating without identity verification (without KYC protocols). This operation, dubbed ‘Operation Final Exchange’, is large-scale and highlights the crucial role played by instant, non-KYC exchange platforms in cybercrime (Menacho-Inga et al., 2025). As their names imply, these sites without KYC protocols have no visible process for collecting users’ identification information before allowing them to deposit or withdraw any amount. They do not ask for names, telephone numbers or email addresses, and do not bother to verify this information before carrying out transactions (Anggriawan & Susila, 2024).

One of the greatest vulnerabilities of the current regulatory framework for crypto-assets is the lack of a central authority with the capacity to supervise and audit transactions. Assigning the supervision and regulation of crypto-assets to non-specialised agencies reduces the effectiveness of these regulations. Furthermore, in the legal sphere, there are no guidelines or prerequisites for obtaining licences to operate in the crypto-asset sector (Hope Kanu, 2025).

From a comparative perspective, the US model presents a fragmented and reactive approach, based on the ex post actions of various agencies. On the other hand, the EU model is characterised by a preventive and harmonised approach, which is geared towards reducing pseudonymity *ex ante*. However, both systems face operational limitations in addressing the international scope of the phenomenon.

Neither system is fully effective. The US model may have gaps in its preventive phase, whilst the European model continues to face challenges in its effective

[10] This stands for *Markets in Crypto-Assets Regulation*, Regulation (EU) 2023/1114 on crypto-asset markets. It is the EU’s first comprehensive regulation governing crypto-assets, their issuers and the service providers associated with them.

implementation and in adapting to the rapid technological evolution of the crypto ecosystem.

8. LEGISLATIVE DEVELOPMENTS IN THE EUROPEAN UNION

The opaque corporate structures used by criminal organisations to launder virtual assets – with the regulation coming into force on 10 July 2027 – will strengthen transparency regarding beneficial ownership, enhance traceability and control over crypto-asset transactions, and prohibit anonymous accounts (Regulation (EU) 2024/1624, Article 79(1)) and will require specific measures for transfers to self-hosted addresses[11] (Regulation (EU) 2024/1624, Article 40).

At the same time, the previous legislative package has been updated by a new Directive on preventive mechanisms, which introduces a state-level obligation to establish mechanisms to identify the person who holds or controls crypto-asset accounts and to interconnect these mechanisms via an EU-wide system (Directive (EU) 2024/1640, Article 16). From a legal perspective, European supervision is strengthened by the creation of the AMLA Authority, which has been fully operational since 1 July 2025 (Regulation (EU) 2024/1620).

8.1. WHAT CHANGES IS THE EU INTRODUCING COMPARED TO THE US TO MITIGATE PSEUDONYMITY AND OPACITY IN THE USE OF CRYPTO-ASSETS?

The EU prohibits crypto-asset service providers from maintaining anonymous accounts or any accounts that allow the account holder to be concealed or that increase the opacity of transactions, specifically mentioning privacy coins (Regulation (EU) 2024/1624, Article 79(1)). In line with this approach, the European PBC/FT package imposes an obligation on crypto-asset service providers to identify and assess risks inherent in transfers involving self-hosted addresses. Similarly, such providers must apply proportionate mitigation measures, which may include identifying and verifying the sender or recipient and collecting additional information on the origin and destination (Regulation (EU) 2024/1624, Article 40(1)). These rules reinforce the objective of limiting the use of crypto-assets for anonymisation purposes, particularly when combined with opaque corporate structures – a context which the European framework itself recognises as giving rise to risks of circumvention and obfuscation, and to which the new 2024 package responds.

The EU has opted to adopt a ‘zero-tolerance’ approach to pseudonymity, with outright bans, uniform rules and a new supranational authority. In contrast, the US follows a decentralised model where anonymity is not prohibited, and the authorities act primarily through criminal or administrative proceedings following the detection of infringements.

[11] A self-hosted address is a cryptocurrency address controlled directly by a user, without the intervention or custody of a regulated intermediary (such as an exchange or a VASP).

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

The key difference is simple. The EU restricts pseudonymisation *ex ante* through prohibitions, whilst the US combats it *ex post* through *enforcement.*[12]

Table 1.
Key differences between the EU and the US regarding pseudonymity and opacity in crypto-assets.

DIMENSION	EU	US
Anonymous accounts.	Explicitly prohibited (Art. 79.1).	Not prohibited by federal law.
Privacy coins	To be banned from 2027.	Not prohibited, but subject to monitoring.
Self-hosted crypto-asset wallets.	Mandatory risk assessment and possible identification. (Art. 40.1).	No federal obligation to identify users.
Regulatory framework.	Comprehensive, unified (MiCA + AMLR).	Fragmented: SEC, CFTC, FinCEN, IRS, states.
Supervision.	Centralised under the AMLA.	Decentralised; each agency acts within its own remit.
Private tokens.	Total elimination.	Not prohibited.
Approach.	Preventive, restrictive, full traceability.	Reactive, punitive, *enforcement-based*.

8.2. WHAT NEW DEVELOPMENTS AFFECT THE IDENTIFICATION OF THE BENEFICIAL OWNER AND CORPORATE TRANSPARENCY IN RELATION TO OPACEOUS STRUCTURES?

Regulation (EU) 2024/1624 specifies the chain of identification of the beneficial owner based on ownership and control, and requires that beneficial ownership information be adequate, accurate and up to date, and that entities report to the central register without undue delay and within a maximum period of 28 calendar days to notify any changes (Regulation (EU) 2024/1624, Article 63). The information required to obtain beneficial owner data is expanded and specified, including, amongst other things, full identification, the nature and extent of the beneficial interest and, where there is a structure involving multiple entities or instruments, a description of the ownership and control structure (Regulation (EU) 2024/1624, Article 62). From a legal perspective, Directive (EU) 2024/1640 lays down rules on the establishment of and access to central beneficial ownership registers and replaces Directive (EU) 2015/849, which is repealed with effect from 10 July 2027 (Directive (EU) 2024/1640; repeal provision).

All of this is in line with the strengthening of the framework for transparency and cooperation across the EU, with the aim of significantly limiting the use of shell companies or opaque corporate structures.

[12] It is an English term meaning ‘application’, ‘execution’ or ‘enforcement’ of the law. In the legal and regulatory sphere, it describes the set of actions, measures and procedures carried out by the competent authorities to ensure that regulations are effectively complied with. In general terms: *enforcement* is the capacity and practice of a state or regulatory authority to investigate, monitor, sanction and rectify regulatory breaches.

In contrast, the United States is facilitating the use of corporate structures by making a U-turn, drastically reducing transparency by removing obligations for US companies, weakening the *Corporate Transparency Act*[13] and leaving transparency in the hands of the states.

Table 2.
Comparison of the framework for beneficial ownership transparency and AML/CFT supervision: European Union vs. United States.

ELEMENT	EUROPEAN UNION	UNITED STATES
Beneficial owner identification chain.	Detailed, comprehensive and mandatory (ownership + control, extent of interest, full corporate structure).	Almost entirely abolished for domestic entities from 2025; applies only to certain foreign entities.[14]
Data updates.	Maximum of 28 calendar days to report changes.	There is no federal obligation for US companies.
Central registers.	Mandatory and harmonised under Directive 2024/1640.	There is no federal register for domestic entities following the 2025 IFR; transparency depends on the states. [15]
Strategy regarding shell companies.	Restrictive, preventative and based on comprehensive traceability.	Regulatory relaxation: the abolition of the federal reporting system facilitates the use of opaque corporate structures.
AML/CFT supervision.	Unified European model under the Anti-Money Laundering Act (AMLA).	Fragmented *enforcement* (FinCEN, IRS, SEC, CFTC), with no single federal framework for beneficial owners.

8.3 LEGAL AND DOCTRINAL IMPLICATIONS OF THE IDENTIFICATION OF THE BENEFICIAL OWNER

From a legal-theoretical perspective, Regulation (EU) 2024/1624 is not merely a reinforcement of formal transparency, insofar as it directly impacts the structural development of the concept of beneficial ownership. This shifts the focus from a purely registrational perspective towards a substantive principle based on effective supervision.

[13] The *Corporate Transparency Act* (CTA) is a US federal law, enacted in 2021, which aims to combat money laundering, terrorist financing, tax fraud and the use of shell companies by requiring the reporting of information on the beneficial owners (*Beneficial Ownership Information*, BOI) of certain entities.
[14] Financial Crimes Enforcement Network. (2025). *Beneficial Ownership Information Reporting. U.S. Department of the Treasury*. https://www.fincen.gov/boi
[15] Weiner, A. J., Montgomery, B. H., Thoren-Peden, D. S., Robbins, R. B., Patay, C. H., Keyko, D. G., & Yee, S. D. (2026). *CTA Update: A review of the status of beneficial ownership reporting requirements under the Corporate Transparency Act and related initiatives as of 5 January 2026.* Pillsbury Winthrop Shaw Pittman LLP. https://www.pillsburylaw.com/en/news-and-insights/cta-update.html

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

From the perspective of economic criminal law, this change is highly significant, as it reduces the scope for indefinite attribution of liability that is characteristic of complex corporate structures. When the identification of the beneficial owner is sought on the basis of both ownership and control, the Regulation establishes a functional criterion that simplifies the legal attribution of liability. It is particularly in money laundering offences where the concealment of the beneficial owner constitutes a central constituent element.

In the same vein, the requirement that information on beneficial ownership be appropriate, accurate and up to date, together with the obligation to notify within a maximum period of 28 days (Article 63), not only has an administrative aspect but also has a direct impact on the probative value of evidence in criminal proceedings. To this end, beneficial ownership registers are established as genuine tools for analysing the financial *crime trail*. This helps to mitigate risk during the investigation phase and facilitates the legal traceability of illicit funds.

The expansion of the information required (Article 62), which includes the nature and extent of beneficial ownership and the analysis of complex structures, introduces a fundamental aspect from the perspective of money laundering doctrine. This makes it possible to establish a legal link between beneficial ownership and the formal appearance of legality. This link is essential for circumventing the conventional limits of criminal law in relation to aspects of asset stratification and segregation, which are common features of money laundering involving crypto-assets.

In line with this approach, Directive (EU) 2024/1640 strengthens the framework for systems of access to and centralisation of information. In this way, it establishes a perspective that goes beyond mere regulatory harmonisation, moving towards a supranational legal framework for transparency. This development entails an optimisation of the principle of administrative and judicial cooperation within the EU, an essential principle in the context of transnational crime.

It can be said that, taken together, these rules create the conditions to sustain the European model by being guided by a preventive and structural approach, aimed not only at punishing conduct but also at limiting, *ex ante*, the conditions under which crime can occur, thereby restricting the use of corporate instruments as mechanisms of opacity.

The US model, by contrast, has significant implications for legal theory. Weakening the *Corporate Transparency Act* and easing the obligations regarding the identification of beneficial owners implies a shift towards a system in which corporate opacity once again becomes a significant area of legal risk. From a legal theory perspective, this complicates the identification of the perpetrator of the offence and makes criminal prosecution more difficult in complex structures.

This stance highlights a structural disparity between the two systems. On the one hand, the EU has developed a model based on *ex ante* identification and legal traceability. Conversely, the US retains a largely reactive approach based on *enforcement*, in which intervention takes place only after the offence has been committed.

From a critical perspective, this divergence is not merely technical, but reflects two distinct conceptions of economic criminal law:

A European model of structural prevention and systemic risk reduction.

An American model of punitive reaction and the prosecution of crime.

In fact, the development of European legislation demonstrates an effort to resolve the conventional disparity between economic traceability and legal attribution. By contrast, the US model continues to face difficulties in integrating both aspects coherently within the sphere of money laundering.

8.4. HOW ARE ACCOUNT TRACING MECHANISMS AND EUROPEAN SUPERVISION BEING STRENGTHENED TO DETECT SCHEMES INVOLVING CRYPTO-ASSETS AND COMPANIES WITH OPAQUE STRUCTURES?

Directive (EU) 2024/1640 requires Member States to establish centralised automated mechanisms enabling the real-time identification of any person who holds or controls, amongst other products, crypto-asset accounts, as well as bank accounts, payment accounts, securities accounts and safe deposit boxes (Directive (EU) 2024/1640, Article 16(1)).

These mechanisms must include minimum information on the account holder, representative, beneficial owner and the dates of opening and closure; for crypto-asset accounts, this must also include a unique identifier and the dates of opening and closure (Directive (EU) 2024/1640, Article 16(3)(f)). Similarly, provision must be made for their interconnection via the BARIS system[16] , which the Commission is to establish and manage, with the aim of achieving interconnection by 10 July 2029 at the latest (Directive (EU) 2024/1640, Article 16(6)).

This strengthening is complemented by the creation of AMLA[17] to oversee and harmonise supervision and make the European system more effective in preventing cross-border risks of money laundering and terrorist financing (Regulation (EU) 2024/1620; general entry into force 1 July 2025), as part of the 2024 European legislative package.

9. EFFECTIVENESS OF THE REGULATORY FRAMEWORK ON MONEY LAUNDERING INVOLVING CRYPTO-ASSETS

The ability to prevent, detect, attribute and sanction money laundering, viewed from the perspective of regulatory effectiveness, requires a comparative examination of these frameworks, insofar as it must also be considered in relation to the principles of legality and legal certainty. The identification of typical offences and their effective investigation depend on the precision of the legislation and the adaptability of economic criminal law in sophisticated technological environments.

---

[16] The *Bank Account Registers Interconnection System* (BARIS) is a Europe-wide computerised system designed to interconnect the national bank account registers of EU Member States, enabling rapid, secure and harmonised access to financial information relevant to the prevention, detection, investigation and prosecution of serious crimes, including money laundering and terrorist financing.

[17] The AMLA (*Anti-Money Laundering Authority* / European Authority for Combating Money Laundering and Terrorist Financing) is a decentralised EU agency, established in 2024 and based in Frankfurt, whose objective is to supervise, coordinate and strengthen compliance with European rules on the prevention of money laundering (AML) and terrorist financing (CFT).

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

Any analysis of the effectiveness of regulatory frameworks concerning money laundering via crypto-assets must move beyond a formal approach centred on the mere existence of rules. Its aim is to assess their actual capacity to prevent, detect and prosecute illicit conduct in a technologically sophisticated environment, as well as the international dimension of this phenomenon. The degree of regulatory development must also be examined in terms of its practical effectiveness and its ability to adapt to the dynamics of the crypto ecosystem.

Based on this premise, it is possible to identify legal and operational criteria for assessing the effectiveness of AML systems in this area.

9.1. PREVENTION CAPACITY

For a system to be effective in policies aimed at preventing and combating money laundering, the first pillar is prevention. In the context of crypto-assets, this first pillar is primarily embodied in the due diligence obligations set out in Article 13 of Directive (EU) 2015/849, relating to know-your-customer (KYC) procedures and risk assessment, with which VASPs must comply.

The EU model takes a more robust approach, offering a harmonised system with clearly defined obligations for intermediaries, thereby strengthening traceability and restricting pseudonymity. The US model, by contrast, faces numerous operational constraints in establishing uniform obligations, which could give rise to areas of risk.

However, preventive effectiveness depends not only on the existence of these obligations, but also on their proper implementation and supervision.

9.2. DETECTION CAPACITY

The detection of suspicious transactions is crucial for mitigating money laundering. In the context of digital currencies, this capability involves the use of *blockchain* analysis tools and collaboration between public and private sector actors.

The traceability or technical tracking of these transactions on public networks does not always result in the effective identification of the participants involved. The effectiveness of regulatory frameworks lies in equipping authorities with technical capabilities and in collaboration with specialised bodies.

9.3. ATTRIBUTION CAPABILITY

As mentioned in the analysis of beneficial ownership, the strengthening of the identification systems set out in Regulation (EU) 2024/1624 helps to bridge the traditional gap between technical traceability and legal attribution. In the BC via crypto-assets, one of the main structural challenges lies in the separation between the traceability of transactions and legal attribution to specific natural or legal persons.

Thus, the requirement for accurate, up-to-date and functionally complete information on the beneficial owner makes it possible to identify links between transactions recorded in decentralised systems—such as the *blockchain* ( )—and specific

legal entities, thereby facilitating criminal prosecution in cases involving decentralised cryptocurrencies.

From a legal theory perspective, these mechanisms enhance the ability to identify the true beneficial owner beyond formal structures, which is of essential importance for establishing the subjective element of the offence and for proving knowledge of the illicit origin of the funds. In this way, the European regulatory framework not only strengthens detection capabilities but also has a decisive impact on the ability to attribute legal liability, overcoming one of the main structural shortcomings of the traditional system in the face of new forms of financial crime based on crypto-assets.

It is necessary to prove the existence of suspicious transactions in order to investigate an offence, its link to a specific individual, and knowledge of the illicit origin of the funds. *Blockchain* networks, together with the use of *mixers*, privacy coins or layering structures, complicate this task due to their pseudonymous nature.

The effectiveness of regulatory frameworks depends on their ability to create points of connection between the digital sphere and the legal world through identification mechanisms and reporting obligations.

9.4. ENFORCEMENT AND SANCTIONING CAPACITY

The final element of assessment concerns the power to investigate, impose sanctions and confiscate illicit assets. This dimension has its own specific characteristics within the field of crypto-assets, such as *blockchain*, cross-border transfers and the operational and technical limitations on their confiscation.

The enforcement-based approach, in line with the US model, is characterised by strong investigative and criminal prosecution capabilities. This reactive nature, however, may not be sufficient unless complemented by preventive measures.

Conversely, we observe a strengthening of the EU's supervisory instruments through the creation of the AMLA, with its effectiveness depending on its capacity to coordinate national authorities.

9.5. COMPARATIVE ASSESSMENT OF EFFECTIVENESS

Having examined this criterion, it is evident that neither model is fully effective on its own. The US system has strengths in sanctions but shortcomings in structural prevention. However, the EU model provides a more coherent and preventive framework, although it faces a structural challenge in its implementation.

For regulatory frameworks to be effective—not merely through legislative development—there must be interaction between regulation, technological capabilities, international cooperation and institutional specialisation. The separation between regulatory planning and operational capacity is the main problem, which reinforces the need for a comprehensive and coordinated approach.

The need for economic criminal law to evolve highlights the importance of striking a balance between the effectiveness of investigations and respect for fundamental rights.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

10. CONCLUSIONS

The analysis carried out throughout this paper confirms that the effectiveness of regulatory frameworks governing money laundering involving crypto-assets does not depend solely on the level of regulatory development. In this regard, it depends on their actual capacity to prevent, detect, attribute and sanction unlawful conduct, by establishing the conditions to affirm that crypto-assets, cryptocurrencies and virtual assets give rise to unique methods, owing to their pseudonymity and the global and decentralised nature of *blockchain* technology, a phenomenon that is expanding. Criminal organisations deliberately exploit these characteristics, using a combination of sophisticated obfuscation techniques (for example, *smurfing*, crypto-asset wallets, mixing services, privacy coins and *cross-chain* bridges) and opaque corporate structures.[18] This serves to fragment, move and conceal the trail of funds, transactions and mixing services, private coins and bridges – vehicles that are susceptible to illicit exploitation to further obscure their tracks. This combination of technological and corporate elements demonstrates that the illicit use of such environments is not accidental, but strategic and deliberate. *Darknet* markets, however, act as facilitators in such cases, providing venues for anonymous trade.

Based on the analysis carried out, it can be stated that money laundering via crypto-assets is a complex phenomenon. It is characterised by the interaction between the technological infrastructure of the digital ecosystem, the international dimension of operations and the adaptability of criminal organisations. The existence of regulatory frameworks in this regard is not sufficient to guarantee their effectiveness.

The US and the EU highlight very different approaches with regard to their regulatory models. Whilst the US model is based on an *enforcement-led* approach, focusing on investigative capacity and the imposition of sanctions, the EU, by contrast, has developed a more harmonised, preventive system aimed at limiting pseudonymity and strengthening the traceability of transactions. Both models, whether in terms of structural prevention or the practical application of the rules, have clear limitations.

The technical traceability of transactions, as noted, does not always translate into the effective identification of the parties involved, which creates significant evidential challenges and limits the legal attribution of the offence. Consequently, the effectiveness of the regulatory framework cannot be measured solely by the degree of regulatory development. It must be assessed on the basis of its actual capacity to prevent, detect, attribute and sanction unlawful conduct.

The notion that effectiveness depends on the integration of supervisory mechanisms, technical capabilities and international cooperation corroborates this reality. The use of third-party crypto-asset wallets, *mixing* services, privacy coins or markets on the *darknet and deep web* demonstrates that the problem lies not solely in pseudonymity, but in the combination of technological, regulatory and institutional factors.

[18] An opaque company is a legal entity whose structure of ownership, control and beneficial ownership is designed to conceal the identity of the persons who actually own or control the company. Its defining characteristic is a lack of transparency, which prevents the identification of *the ultimate beneficial owner* (UBO).

Institutional efforts to mitigate money laundering through crypto-assets require a comprehensive approach that combines regulation, technology and operational capacity, bridging the gap between regulatory design and its effective implementation. Through this interaction, it becomes easier to strengthen prevention, detection and prosecution in the crypto-asset environment, given that none of the models examined are fully effective on their own.

The main contribution of this study lies in having identified the disconnect between technological traceability and legal attribution as the central issue underpinning the current limitations of the ML prevention system for crypto-assets.

11. FINAL REFLECTIONS

The study of money laundering through crypto-assets highlights a phenomenon that goes beyond the traditional categories of criminal law and financial regulation. Technological developments have brought with them not only opportunities for innovation and new forms of value circulation, but also the potential to create areas of risk that are difficult to reconcile with existing regulatory models.

This comparative study demonstrates that neither an *enforcement-centred* approach nor a predominantly preventive model is sufficient on its own, as it is necessary to rethink conventional mechanisms of legal intervention. The ability of legal systems to adapt to an environment characterised by speed, decentralisation and technical complexity is the new challenge we are forced to face, as is the need for more modern regulations.

In the context of crypto-assets—which reflect a growing tension between technical traceability and legal attribution, and between formal regulation and operational effectiveness—the Central Bank goes beyond the divergences between jurisdictions. The new role of institutions necessitates a re-evaluation of this emerging tension, international cooperation and the integration of technological capabilities as essential elements of the system.

The definitive institutional response to mitigate this phenomenon cannot be solely regulatory, but must also be technological. A comprehensive approach will help bridge the gap between the development of regulations and their efficient implementation, ensuring a coherent legal response to a constantly evolving phenomenon.

12. REFERENCES

Anggriawan, R., & Susila, M. (2024). Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations. *Novum Jus, 18(2)*. Available at: https://doi.org/10.14718/novumjus.2024.18.2.10 [Last accessed: 23/02/2026].

Akkoyun, A. G., & Çelik, M. E. (2022). Transnational Organised Crime and the UN Convention. *Frontiers in Law, 1, 9–21*. Available at: https://doi.org/10.6000/2817-2302.2022.01.02 [Last accessed: 23/02/2026].

Alessi Longa, F. (2025). Cryptocurrency and money laundering. *American Journal of Industrial and Business Management, 15(2), 362–371*. Available at: https://doi.org/10.4236/ajibm.2025.152017 [Last accessed: 23/02/2026].

Anguren, R., García Alcorta, J., García Calvo, L., Hernández García, D., & Valdeolivas, E. (2023). The regulation of crypto-assets within the current international and European framework. *Journal of Financial Stability*, 44, Bank of Spain. Available at: https://doi.org/10.53479/30054 [Last accessed: 23/02/2026].

Arnone, G., Scirè, G., & Bivona, E. (2025). The (mis)use of cryptocurrencies by criminal organisations: a systematic literature review. *Digital Finance, 7, 815–851*. Available at: https://doi.org/10.1007/s42521-025-00148-1 [Last accessed: 23/02/2026].

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review. *Electronics, 13(17), 3568*. Available at: https://doi.org/10.3390/electronics13173568 [Last accessed: 23/02/2026].

Baer, K., de Mooij, R., Hebous, S., & Keen, M. (2023). Taxing cryptocurrencies. *Oxford Review of Economic Policy, 39(3), 478–497*. Available at: https://doi.org/10.1093/oxrep/grad035 [Last accessed: 23/02/2026].

Béres, F., Seres, I. A., Benczúr, A. A., & Quintyne-Collins, M. (2021). Blockchain is Watching You: Profiling and Deanonymising Ethereum Users. *2021 IEEE International Conference on Decentralised Applications and Infrastructures (DAPPS), 69–78*. Available at: https://doi.org/10.48550/arXiv.2005.14051 [Last accessed: 23/02/2026].

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access, 9, 61048–61073*. Available at: https://doi.org/10.1109/ACCESS.2021.3072849 [Last accessed: 23/02/2026].

Blanco Barón, C. (2025). The regulation of crypto-assets: beyond a question of efficiency. *Revista de Economía Institucional, 27(53), 133–186*. Available at: https://doi.org/10.18601/01245996.v27n53.07 [Last accessed: 23/02/2026].

Chiang, S. (2024). Crypto Is Increasingly Being Used for Money Laundering. CNBC. Available at: https://www.cnbc.com/2024/07/16/crypto-is-increasingly-being-used-for-money-laundering-chainalysis-says.html [Last accessed: 23/02/2026].

Cremers, C., Loss, J., & Wagner, B. (2024). A holistic security analysis of Monero transactions. In Advances in Cryptology – EUROCRYPT 2024 (pp. 129–159). *Springer*. Available at: https://doi.org/10.1007/978-3-031-58734-4_5 [Last accessed: 23/02/2026].

Enríquez Pérez, I. (2020). Organised crime and institutional fragility as conditioning factors for development. *Revista Facultad de Ciencias Económicas*, 28(1). Available at: https://doi.org/10.18359/rfce.3564 [Last accessed: 23/02/2026].

Farrukh, H., Zafar, S., Rehman, Z. U., Shah, A. A., & Alshammry, N. (2025). Blockchain-based fraud detection: A comparative systematic literature review of federated learning and machine learning approaches. *Electronics*, 14(24), 4952. Available at: https://doi.org/10.3390/electronics14244952 [Last accessed: 23/02/2026].

Fu, Q., Liu, J., Pan, S., & Yuen, T. H. (2025). SoK: A deep dive into AML techniques for blockchain cryptocurrencies. *In ACISP 2025*. Available at: https://doi.org/10.1007/978-981-96-9095-4_16 [Last accessed: 23/02/2026].

Gorjón, S. (2023). Decentralised finance or next-generation crypto-assets. *Economic Bulletin 2023/Q3*, art. 04. Available at: https://doi.org/10.53479/30650 [Last accessed: 23/02/2026].

Hemdani, M. G. K. (2025). Cryptocurrencies and the Dark Web: A Gateway to Money Laundering. In *Cybercrime Unveiled: Technologies for Analysing Legal Complexity* (pp. 217–247). *Springer*. Available at: https://doi.org/10.1007/978-3-031-80557-8_10 [Last accessed: 23/02/2026].

Hinojal, A. (2023). Cryptocurrencies and money laundering. *Logos Guardia Civil, 1, 215–240.* Available at: revistacugc.es/article/view/5742 [Last accessed: 23/02/2026].

Holt, T. J., Lee, J. R., & Griffith, E. (2023). An Assessment of Cryptomixing Services in Online Illicit Markets. *Journal of Contemporary Criminal Justice*. Available at: https://doi.org/10.1177/10439862231158004 [Last accessed: 23/02/2026].

Hope Kanu, D. (2025). Regulation of cryptocurrency and its implications for financial stability: A qualitative analysis. *IJEBMR, 9(4).* Available at: https://doi.org/10.51505/IJEBMR.2025.9416 [Last accessed: 23/02/2026].

Isolauri, E. A., & Ameer, I. (2023). Money laundering as a transnational business phenomenon: A systematic review and future agenda. *Critical Perspectives on International Business, 19(3), 426–468.* Available at: https://doi.org/10.1108/cpoib-10-2021-0088 [Last accessed: 23/02/2026].

Jordá, C., Píriz, C., & Giménez-Salinas, A. (2024). Illicit cryptocurrency markets for drug trafficking on the Dark Web: an exploratory empirical study. *Revista Española de*

Investigación Criminológica, 22(2). Available at: https://doi.org/10.46381/reic.v22i2.884 [Last accessed: 23/02/2026].

Kabra, S., & Gori, S. (2025). Combating Cryptocurrency Laundering by Organised Crime Groups through an Effective Regulatory Framework. *IIUM Law Journal, 33(1)*. Available at: https://doi.org/10.31436/iiumlj.v33i1.1007 [Last accessed: 23/02/2026].

Koelbing, M., Kieseberg, K., Çulha, C., Garn, B., & Simos, D. E. (2024). Modelling smurfing patterns in cryptocurrencies using integer partitions. *IET Blockchain*. Available at: https://doi.org/10.1049/blc2.12087 [Last accessed: 23/02/2026].

Langdale, J. (2024). Combatting money laundering in Southeast Asian and Australian casinos. In Financial Crime and the Law (pp. 225–245). *Springer*. Available at: https://doi.org/10.1007/978-3-031-59543-1_9 [Last accessed: 23/02/2026].

Legrand, T., & Leuprecht, C. (2021). Securing Cross-Border Collaboration: Transgovernmental Enforcement Networks. *Policy and Society*, 40(4), 565–586. Available at: https://doi.org/10.1080/14494035.2021.1975216 [Last accessed: 23/02/2026].

Lim, A., & Choi, K.-S. (2025). Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimisation. *International Journal of Cybersecurity Intelligence & Cybercrime, 8(2).* Available at: https://doi.org/10.52306/2578-3289.1220 [Last accessed: 23/02/2026].

Lom, A., & Hashmall, R. (2021). *New FATF Guidance Released on Virtual Assets and VASPs*. Available at: https://www.nortonrosefulbright.com/en-us/knowledge/publications/024b3d80/new-fatf-guidance-released-on-virtual-assets-and-virtual-asset-service-providers [Last accessed: 23/02/2026].

Luna Galván, M., Luong, H. T., & Astolfi, E. (2021). Drug trafficking as organised crime: a transnational and multidimensional perspective. *Journal of International Relations, Strategy and Security, 16(1).* Available at: https://doi.org/10.18359/ries.5412 [Last accessed: 23/02/2026].

Medranda Morales, N., & Arcos Argudo, M. (2023). Crypto-assets and cryptocurrencies. In Blockchain, crypto-assets and the metaverse (pp. 41–62). *Abya-Yala Publishers*. Available at: https://doi.org/10.17163/abyaups.6 [Last accessed: 23/02/2026].

Menacho-Inga, W. G., Proaño-Reyes, G., & Castro-Sánchez, F. (2025). The use of cryptocurrencies and money laundering in Ecuador. *Noesis, 7(esp2)*. Available at: https://doi.org/10.35381/noesisin.v7i2.620 [Last accessed: 23/02/2026].

Mollaahmetoğlu, M. B., & Baykut, C. (2021). *Financial Action Task Force's Updated Guidance*. Available at: https://chambers.com/articles/financial-action-task-force-s-updated-guidance-virtual-assets-and-virtual-asset-service-providers [Last accessed: 23/02/2026].

Montoya Arrubla, E. (2025). *Mechanisms for controlling crypto-asset money laundering*. Diálogos Punitivos. Available at: https://dialogospunitivos.com/wp-content/uploads/2025/04/Columna-de-interes-43.pdf [Last accessed: 23/02/2026].

Rodríguez-Valencia, L., et al. (2025). A systematic review of artificial intelligence applied to compliance: fraud detection in cryptocurrency transactions. *Journal of Risk and Financial Management, 18(11), 612*. Available at: https://doi.org/10.3390/jrfm18110612 [Last accessed: 23/02/2026].

Soltani, R., Zaman, M., Joshi, R., & Sampalli, S. (2022). Distributed Ledger Technologies and Their Applications: A Review. *Applied Sciences, 12(15), 7898.* Available at: https://doi.org/10.3390/app12157898 [Last accessed: 23/02/2026].

Sudan, H. K., Tai, A. M. Y., Kim, J., & Krausz, R. (2023). Decrypting the cryptomarkets. Drug Science, *Policy and Law, 9, 1–19*. Available at: https://doi.org/10.1177/20503245231215668 [Last accessed: 23/02/2026].

Teng, H.-W., Härdle, W. K., Osterrieder, J., Pele, D. T., Baals, L. J., Papavassiliou, V.,

Bolesta, K., Kabašinskas, A., Filipovska, O., Thomaidis, N. S., Moukas, A.-I., Goundar, S., Abdul Nasir, J., Weinberg, A. I., Arakelian, V., Truică, C.-O., Akar, M., Kabaklarlı, E., Apostol, E.-S., Iannario, M., Będowska-Sójka, B., Skaftadóttir, H. K., Yildirim, O., Shala, A., Pisoni, G., Coita, I. F., Korba, S., Hafner, C. M., Schwendner, P., Molnár, B., & Xhumari, E. (2026). Digital assets: risks, regulations, mitigation. *Financial Innovation, 12, 65*. Available at: https://doi.org/10.1186/s40854-025-00848-y [Last accessed: 23/02/2026].

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science, 11(1)*. Available at: https://doi.org/10.1186/s40163-021-00163-8 [Last accessed: 23/02/2026].

Wang, H.-M., & Hsieh, M.-L. (2023). Cryptocurrency is the new trend: a reflection on money laundering prevention. *Security Journal, 37, 25–46*. Available at: https://doi.org/10.1057/s41284-023-00366-5 [Last accessed: 23/02/2026].

Warren, E., & Marshall, R. (2022). *Digital Asset Anti-Money Laundering Act of 2022 (S.5267)*. United States Senate. Available at: https://www.congress.gov/bill/117th-congress/senate-bill/5267 [Last accessed: 23/02/2026].

13. REPORTS BY ORGANISATIONS

AMLC. (2023). *Analysis of Suspicious Transactions Associated with Casino Junkets*. Available at: http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf [Last accessed: 23/02/2026].

DEA. (2025). *National Drug Threat Assessment 2025*. Available at: https://www.dea.gov/documents/2025/2025-05/2025-05-13/national-drug-threat-assessment [Last accessed: 23 February 2026].

Europol. (2024). *Cryptocurrencies – Tracing the Evolution of Criminal Finances*. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf [Last accessed: 23/02/2026].

Europol. (2022). Cryptocurrencies: Tracing the evolution of criminal finances. *Europol Spotlight Series*. Available at: https://doi.org/10.2813/75468 [Last accessed: 23/02/2026].

FATF, Egmont Group, INTERPOL, & UNODC. (2025). *International cooperation on money laundering detection, investigation and prosecution: Handbook*. Paris: FATF. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html [Last accessed: 23/02/2026].

FATF. (2024). *Virtual assets: FATF standards and implementation*. FATF. Available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Last accessed: 23/02/2026].

FATF. (2023). *Targeted Update on Implementation of FATF Standards on Virtual Assets and VASPs*. FATF. Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html [Last accessed: 23/02/2026].

FATF.1. (2023). *Virtual Assets: Global* FATF Standards. Available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html [Last accessed: 23/02/2026].

FATF. (2022). *Money Laundering from Fentanyl and Synthetic Opioids*. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Fentanyl-Synthetic-Opioids.pdf.coredownload.inline.pdf [Last accessed: 23/02/2026].

FATF. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf [Last accessed: 23/02/2026].

FinCEN. (2025). *Advisory on Chinese Money Laundering Networks*. Available at: https://www.fincen.gov/news/news-releases/fincen-issues-advisory-and-financial-trend-analysis-chinese-money-laundering [Last accessed: 23/02/2026].

Ministry of the Interior. (15 November 2024). *Joint operation by the Spanish National Police and the Dutch Nationale Politie (OTC method)*. Available at:

https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16371# [Last accessed: 23/02/2026].

NYDFS. New York State Department of Financial Services. (2024–2026). *Virtual Currency Business Licensing.* Available at: https://www.dfs.ny.gov/virtual_currency_businesses [Last accessed: 23/02/2026].

UNODC. (2026). *Global Programme on Cybercrime (capacity-building materials)*. Capacities/training on cryptocurrency, the darknet and digital evidence: Available at: https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/detectandrespond/capacitybuilding.html. 2024 Training Catalogue: https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf [Last accessed: 23/02/2026].

UNODC. (2025). *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces.* Available at: https://www.unodc.org/roseap/en/2025/04/cyberfraud-inflection-point-mekong/story.html [Last accessed: 23/02/2026].

UNODC. (2024). *Annual Report 2024: Organised Crime Section. United Nations Office on Drugs and Crime*. Available at: https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Last accessed: 23/02/2026].

UNODC.1. (2024). *Criminal Networks and Fragmented Structures*. Available at: https://www.unodc.org/documents/AnnualReport/UNODC_REPORT_2024_MAY6_WEB.pdf [Last accessed: 23/02/2026].

UNODC.2. (2024). *Casinos, Money Laundering, Underground Banking and Transnational Organised Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. Available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf [Last accessed: 23/02/2026].

U.S. Department of Justice. (2023). *United States v. Binance Holdings Limited, d/b/a Binance.com (case overview).* Available at: https://www.justice.gov/criminal/case/united-states-v-binance-holdings-limited-dba-binancecom [Last accessed: 23/02/2026].

U.S. Department of Justice.1. (2023). *United States v. Changpeng Zhao (case overview)*. Available at: https://www.justice.gov/criminal/case/united-states-v-changpeng-zhao [Last accessed: 23/02/2026].

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004

14. LEGISLATION

Council of the European Union. (2024) Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be established 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. OJEU L 2024/1640, 19 June 2024.

United Nations. (2000). United Nations. (2000). United Nations Convention against Transnational Organised Crime (Resolution A/RES/55/25).

European Parliament. (2024). Sixth Anti-Money Laundering Directive. Legislative Resolution of the European Parliament of 24 April 2024 on the proposal for a Directive on measures to prevent the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849. OJEU C/2025/3790, 17 September 2025.

European Parliament and Council of the European Union. (2024) 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. OJ L 2024/1624, 19 June 2024.

European Parliament and Council of the European Union. (2024) Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024, establishing the Anti-Money Laundering and Counter-Terrorist Financing Authority and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010. OJEU L 2024/1620, 19 June 2024

European Parliament and Council of the European Union. (2023) 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. OJEU, L 150, 9 June 2023.

United States Congress. (1977). International Emergency Economic Powers Act, Pub. L. No. 95-223, 91 Stat. 1625–1629 (codified, as amended, in 50 U.S.C. §§ 1701–1707).

United States Congress. (1970). Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114

(codified, as amended, at 31 U.S.C. §§ 5311–5336).

15. OTHER NON-SCIENTIFIC SOURCES

Binance Academy. (2024). What is cryptocurrency mining and how does it work? Binance. Available at: https://www.binance.com/es/academy/articles/what-is-crypto-mining-and-how-does-it-work [Last accessed: 23/02/2026].

Chainalysis. (2025). 2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalised. Available at: https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/ [Last accessed: 23/02/2026].

Coinmetro Editorial Team. (2 August 2024). Crypto Mixers: Privacy Tools and Regulatory Challenges. *Coinmetro*. Available at: https://coinmetro.com/learning-lab/crypto-mixers-privacy-tools-and-regulatory-challenges [Last accessed: 23/02/2026].

Elliptic. (2024). *Preventing Financial Crime in Cryptoassets: Typologies Report.* https://www.elliptic.co/hubfs/Elliptic%20Typologies%20Report%202024.pdf [Last accessed: 23/02/2026].

16. DECLARATION OF ACADEMIC AND SCIENTIFIC INTEGRITY

This constitutes an original piece of work, carried out by me, without plagiarism or the improper use of others' work, in accordance with international standards of academic and scientific integrity.

The data, results and conclusions have been obtained and analysed honestly and rigorously, without fabrication, falsification or improper manipulation.

The use of artificial intelligence or other digital tools has complied with university regulations, without substituting intellectual authorship or my own academic judgement.

There are no conflicts of interest that have influenced the conduct or results of the research.

I am aware that failure to comply with these declarations may result in the revocation of my doctoral degree and may give rise to the relevant academic or legal liabilities.

I hereby ASSUME any liability arising from a breach of the ethical commitment set out in this declaration.

doi: https://doi.org/10.64217/logosguardiacivil.v4i2.8913
https://orcid.org/0009-0005-6923-1004