BANCA D'ITALIA
EUROSISTEMA

Crypto-assets, Stablecoins, and Anti-Money Laundering

Paolo Angelini
Deputy Governor of Banca d'Italia

Opening Remarks at the 5th UIF-Bocconi Workshop
"Quantitative Methods and the Fight Against Economic Crime"

Rome, 28 November 2025

1. Introduction

It is with great pleasure that I welcome you to the fifth edition of the conference on "Quantitative Methods and the Fight Against Economic Crime", an initiative jointly launched in 2015 by the Financial Intelligence Unit (UIF) of Italy and the Baffi Center at Bocconi University.

The size of the criminal economy is very difficult to measure and highly uncertain. According to the most recent estimates by ISTAT, the shadow economy and illegal activities generated € 218 billion of value added in 2023, equal to 10 percent of GDP. Based on an experimental mapping conducted by the UIF, 2 percent of the firms operating in the Italian economy during the 2011-2020 decade are estimated to have had potential links to mafia organizations.[1] And about 15 percent out of the approximately 145,000 suspicious transaction reports (STR) received by the UIF last year showed connections between businesses and organized crime.[2]

The actions of mafia groups entail significant economic and social costs.[3] In the past decade, substantial progress has been made thanks to a multi-pronged strategy that has involved economic development measures, investigative and judicial actions, and targeted preventive measures, especially in the financial sector.

---

1 See Rapporto Annuale della UIF sul 2020, pp. 47-48; J. Arellano-Bover *et al.* (2024), "Mafias and firms", Quaderni dell'antiriciclaggio n. 24, Unità di Informazione Finanziaria.

2 A further eighteen per cent of reports feature potential links to organized crime, identified through the so-called 'coordinated' STRs: Unità di Informazione Finanziaria (2025), "Rapporto Annuale sul 2024".

3 F. Panetta (2025), "Costruire la legalità economica: istituzioni, riforme, tecnologia", Opening remarks at the Inaugurazione dell'Anno di Studi 2025-26 of the Scuola di Polizia Economico-Finanziaria.

These initiatives can be strongly supported by technology and research, as today's presentations will demonstrate. Technology, however, can also facilitate criminal activity, and criminals in fact use it skillfully. Below, after briefly touching on new trends in organized crime, I will focus on the use of crypto-assets for illegal purposes.

2. New trends in organised crime

The integration of assets from criminal activities into the legal economy have characterized the entire history of illegality. The phenomenon is not easy to measure: reliable data for comparisons over time or across countries are not available.[4] Globalization has been accompanied by the transnational expansion of criminal organizations. More recently, as international relations have deteriorated, growing connections have emerged between criminal activities and States.

A second point of relevance is related to the use of new technologies for illegal purposes, not only in the digital sphere, such as the continuous introduction of new synthetic drugs onto the market, the use of 3D printing for the production of weapons, and the use of drones for drug trafficking.[5] Some criminal groups are engaged in large-scale, industrial-level cyber fraud.[6] One manifestation of this trend is payment fraud targeting bank customers. Such fraud is on the rise in Italy in recent years, although its value remains stable relative to the total volume of transactions. Recently, several online customer identification procedures used by banks have been circumvented through the use of altered real images or entirely synthetic ones.

Another significant trend is the specialization of illicit activities according to crime-as-a-service and fraud-as-a-service models, with the establishment of international networks specializing by activity and macro-geographic area to provide services to the crime and fraud industry.[7]

At the same time, illegal markets continue to expand. The number of consumers of psychotropic substances – who fuel a highly profitable market for criminal organizations – is estimated to have increased by 29 percent between 2013 and 2023.[8]

---

4 According to some sources, in 2024 the profits of organized crime were estimated to amount to five per cent of global GDP. See The Millennium Project. For evidence regarding Italy, see the Financial Security Committee's "Analisi Nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo", November 2024.

5 See G. Melillo, "Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere", Audizione del 21 giugno 2023; Europol (2024), "EU Drug Market Analysis"; Europol (2025), "The changing DNA of serious and organized crime"; P. Williams (2024), "The fifth wave - Organized crime in 2040", Global Initiative against Transnational Organized Crime.

6 See The Economist, "The vast and sophisticated global enterprise that is Scam Inc", 6 February 2025; Global Initiative against Transnational Organized Crime (2025), "Compound crime - Cyber scam operations in Southeast Asia".

7 See Europol (2013 and 2017), "European Union Serious And Organised Crime Threat Assessment".

8 The figure refers to the population aged between 15 and 64, which is estimated to have increased from 246 million in 2013 to 316 million in 2023 (UNODC World Drug Report, 2025, accessed on 31 October).

3. Developments in the world of finance and payments

This set of illegal activities generates its own demand for financial and payment services, which benefits from the digital revolution in the financial system.[9] In this context, the use of crypto-assets for money laundering and terrorist financing is of great interest. This is not a new phenomenon, but it is evolving in ways that are worth exploring from multiple perspectives, including AML/CFT.

The fight against the illicit use of crypto-assets occurs primarily through the regulation of specialized intermediaries, who handle the majority of crypto-asset transactions. These intermediaries, originally created to safeguard clients' bitcoins and to enable conversion into legal currency and vice-versa, have gradually expanded their offerings to include hundreds of tokens and more complex trading and investment services. Under the leadership of the Financial Action Task Force (FATF), major jurisdictions have introduced regulations for these operators. In the EU, MiCAR has established the category of crypto-asset service providers (CASPs), who are required to comply with AML/CFT rules similar to those applied to traditional financial intermediaries. Similar provisions exist in various countries, including the United States.

Overall, although regulation remains far from the desirable degree of international harmonization, efforts to counter the illegal use of crypto-assets through the regulation of specialized intermediaries appear to be underway.

Precisely due to regulatory heterogeneity, the role of traditional intermediaries remains important. For example, a European user might attempt to bypass MiCAR controls by operating on crypto-platforms located in more permissive jurisdictions. However, he would not be able to avoid the controls imposed by banking institutions when requesting that the foreign platform convert crypto-assets into legal currency and transfer the funds to an account within the EU. In this domain, therefore, traditional mechanisms for combating illegal activity are already active and require conceptually simple-though practically complex-adaptations.

From an AML/CFT perspective, crypto-assets nonetheless pose specific challenges that are not easy to overcome. The most evident is the possibility of transferring these instruments without specialized intermediaries. It is well-known that crypto-assets were born with the intention of eliminating financial intermediation and can be exchanged directly between private individuals through so-called unhosted (or self-custodial) wallets. These are combinations of software and hardware, readily available, that allow users to hold and use their crypto-assets directly without being subject to customer due diligence by intermediaries, thereby operating on blockchains in a pseudo-anonymous

---

9 F. Panetta, "Moneta e fiducia, dal Rinascimento all'era digitale", 2025; P. Cipollone, Opening remarks at the Conference "The future of payments: CBDC, digital assets and digital capital markets" organized by Bocconi University, the Centre for Economic Policy Research, and the European Central Bank, 2025.

manner;[10] they differ from hosted (custodial) wallets, which are managed by a CASP and therefore subject to AML/CFT regulation.[11]

Today, therefore, a criminal can replace the classic briefcase filled with high-denomination banknotes with a self-custodial wallet – a sort of "electronic briefcase" – that can contain far greater value and can be conveniently stored and transported on a device resembling a USB key with advanced encryption, or even on a mobile phone.

In this context, the phenomenon of stablecoins becomes relevant: crypto-assets generally issued by an identifiable entity, designed to maintain a stable value pegged to one or more assets – typically an official currency – and thus allowing criminals to minimize the risks associated with the high volatility of other crypto-assets (such as Bitcoin). The "electronic briefcase" can therefore contain monetary amounts that are not only extremely large, but also essentially stable. Stablecoins thus represent a "red risk" for the anti–money laundering and organized crime prevention system.

Efforts to counter the illegal use of self-custodial wallets remain at an early stage. European law requires CASPs to adopt measures to verify the identity of users interacting with self-custodial wallets.[12] Preliminary discussions between supervisory authorities and Italian CASPs indicate that CASPs are adopting measures to mitigate risks arising from the use of these instruments, including mechanisms based on whitelists of authorized wallets, as well as analytical tools capable of examining public blockchain ledgers. These tools help identify suspicious transactions, such as those linked to cybercriminal groups, sanctioned entities, or operators and individuals in high-risk jurisdictions.

Another approach to combating the illegal use of self-custodial wallets relies on the issuers of crypto-assets themselves. These issuers can not only monitor transactions recorded on public blockchains (similarly to CASPs, law enforcement, or any other technically capable actor); under certain conditions, they can also block or recover crypto-assets used in suspicious or illicit activities, even when held in self-custodial wallets.[13] It is to be hoped that clear provisions regulating the powers of issuers will complement the obligations imposed on crypto-asset service providers. Such provisions are not present in current

---

10 Transactions recorded on public blockchains are freely accessible, but they involve so-called 'virtual addresses', random alphanumeric strings that do not contain useful information for directly tracing the identity or location of their users. However, in some cases it is possible, by analyzing the transactions, to identify addresses potentially controlled by the same entity (the so-called 'clustering') and to de-anonymize them when additional information is available that can link them to real identities (e.g. through listing by authorities or the sharing of an address on a social media profile).

11 Self-custodied wallets, while exposing users to greater risks (for example, the loss of the keys needed to unlock the crypto-assets held, or theft or damage to the hardware), offer higher levels of anonymity as well as greater autonomy in management and, in some cases, lower usage costs.

12 See Regulation (EU) 2023/1113, also known as the recast of the Transfer of Funds Regulation (TFR).

13 This under the condition that the issuer has provided for such a possibility in the smart contracts governing the issuance and circulation of a token. For these purposes, knowledge of the private keys of self-custodied wallets would not be required, whereas such knowledge is necessary for the seizure of crypto-assets without an issuer (such as Bitcoin).

EU legislation, though they are being introduced or discussed in other jurisdictions, including the United States.[14]

Nonetheless, transactions conducted exclusively through self-custodial wallets, without passing through the blockchain, evade the control of both issuers and specialized operators.[15] Moreover, although still limited in Europe, decentralized finance ("DeFi") schemes are spreading, in which crypto-asset services are provided without CASPs and therefore without AML/CFT safeguards.[16]

Today, virtually all stablecoins in circulation are denominated in U.S. dollars and issued by two entities: Tether International S.A. and Circle. Tether is legally headquartered in El Salvador and is not authorized under EU or U.S. regulation.[17] In Europe, Tether-issued stablecoins cannot be traded by CASPs, and their exchanges are subject to limited AML/CFT oversight within the EU;[18] such safeguards apply to transactions in stablecoins issued by Circle[19] (which complies with MiCAR), but only when transactions occur via CASPs.

The current stock of stablecoins in circulation is valued at approximately $ 310 billion – a significant absolute amount but negligible when compared, for example, with U.S. bank deposits (1.5 percent).[20] The intense international debate surrounding stablecoin risks is motivated by concerns about their potential growth. Euro-denominated stablecoins distributed by major technology firms, which have access to massive customer bases, could quickly achieve a level of acceptance not far from that of traditional payment

---

14 The Genius Act contains references to the AML/CFT framework applicable to authorized stablecoin issuers; in this context, for example, it mentions 'technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations.' In the United Kingdom, a recently published consultation paper by the Bank of England on the regulation of systemically important stablecoins provides for the application of AML/CFT obligations within the token redemption process; AML/CFT obligations for issuers of other stablecoins were proposed in May 2025 by the Financial Conduct Authority, the competent authority in this field.

15 These are transactions carried out through the transfer of the private cryptographic key, without any record being entered on the blockchain.

16 See ESMA and EBA, "Recent developments in crypto-assets (Article 142 of MiCAR)".

17 According to the official assessments of GAFILAT, the regional body of the FATF, El Salvador's AML/CTF system showed progress in 2024 but retains significant shortcomings, particularly in the area of supervision.

18 As highlighted by ESMA, CASPs cannot offer to the public nor trade crypto-assets (ARTs or EMTs) that do not comply with the requirements laid down in MiCAR; however, they may handle the transfer of such assets to or from third parties, as well as their custody, and therefore AML/CFT safeguards apply to these services.

19 USDC is issued under a 'multi-issuer' scheme by the U.S. company Circle Internet Financial LLC and the French company Circle Internet Financial Europe SAS, using the same trade name. The latter is subject to MiCAR and to ACPR's supervision.

20 Based on the information available, these stablecoins are used predominantly for transactions involving other crypto-assets. Illicit uses fall within this category, although they presumably do not exhaust it. There is also evidence of the use of stablecoins in countries affected by monetary instability, where demand for assets not subject to loss of value is relatively strong. Finally, there is anecdotal evidence of a third use, namely for remittances by emigrants. See, for example, R. Auer, U. Lewrick and J. Paulick (2025), 'DeFying Gravity? An Empirical Analysis of Cross-Border Bitcoin, Ether and Stablecoin Flows', BIS Working Papers No. 1265; I. Alsadoro, M. Aquilina, U. Lewrick and S.H. Lim (2025), 'Stablecoin growth – policy challenges and approaches', BIS Bulletin No. 108.

instruments. Should this occur, the need to convert the proceeds of crime into traditional instruments could diminish, or even disappear. The challenges this would create for combating illegal activities are evident. It would also pose risks to financial stability, which I will not address here.[21]

The FATF's Virtual Asset Contact Group is working on analyzing and mitigating AML/CFT risks related to stablecoins and decentralized finance;[22] dedicated reports will be published on these topics, which may provide the impetus to strengthen preventive measures and reduce opportunities for regulatory arbitrage.

4. Conclusions

Technological progress is exploited both by the criminal industry and by the system tasked with combating it. Banca d'Italia, and UIF in particular, possess extensive, unique and internationally recognized datasets that make it possible to model behaviors, identify risk areas, and assess the extent of criminal infiltration across sectors, taking into account not only economic interests but also the relational dimension of criminal phenomena. Some results of this work will be presented throughout the day.

These studies show that quantitative methods, combined with high-quality microdata, can significantly increase the efficiency and effectiveness of the UIF's actions, offsetting the increasing sophistication and complexity of the techniques used by criminal organizations to evade controls.

For the system to function effectively in combating illegality, all actors are required to share techniques, information and results and, more broadly, to foster strategic interaction and collaboration: supervisory authorities, investigative bodies, judicial authorities, financial intermediaries, and the research community. Today's initiative aims to pursue this objective and testifies to our institutions' and our enterprises' commitment to safeguarding the integrity and legality of the economic system.

---

21 In the current debate, attention is drawn to the risks of redemption runs and to those inherent in schemes that issue the same instrument through issuers incorporated in different countries; see, for example, Financial Stability Board, 'FSB Plenary sets out 2026 work plan', 2025; Banca d'Italia, Financial Stability Report, No. 2, 2025.

22 See FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers", June 2025.

Designed by the Printing and Publishing Division of Banca d'Italia