



BANCA D'ITALIA
EUROSISTEMA

Criptoattività, stablecoin e antiriciclaggio

Paolo Angelini

Vice Direttore generale della Banca d'Italia

Intervento introduttivo al V Workshop UIF-Bocconi

"Metodi quantitativi e contrasto alla criminalità economica"

Roma, 28 novembre 2025

1. Premessa

È con grande piacere che vi do il benvenuto alla quinta edizione del convegno su "Metodi quantitativi e contrasto alla criminalità economica", un'iniziativa avviata congiuntamente nel 2015 dall'Unità di Informazione Finanziaria (UIF) della Banca d'Italia e dal Centro Baffi dell'Università Bocconi.

Le dimensioni dell'economia criminale sono assai difficili da misurare, e assai incerte. Secondo le più recenti stime dell'Istat l'economia sommersa e le attività illegali hanno generato nel 2023 un valore aggiunto pari a 218 miliardi di euro e al 10 per cento del PIL. Sulla base di una mappatura sperimentale della UIF, il 2 per cento delle imprese operanti nell'economia italiana nel decennio 2011-2020 avrebbe avuto potenziali collegamenti con le mafie¹. Delle oltre 145.000 segnalazioni di operazioni sospette ricevute dalla UIF l'anno scorso, circa il 15 per cento ha mostrato connessioni tra le imprese e la criminalità organizzata².

L'azione delle mafie comporta costi economici e sociali rilevanti³. Nell'ultimo decennio sono stati realizzati notevoli progressi grazie a una politica di contrasto che ha agito su più fronti, con misure per lo sviluppo economico, azioni a livello investigativo e giudiziario, puntuali misure di prevenzione, soprattutto in ambito finanziario.

¹ Cfr. il [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 queste si aggiunge un ulteriore 18 per cento di segnalazioni con potenziali collegamenti di contesto con la criminalità organizzata rilevati dalle SOS cd. 'raccordate'. Unità di Informazione Finanziaria (2025), ["Rapporto Annuale sul 2024"](#).

³ F. Panetta (2025), ["Costruire la legalità economica: istituzioni, riforme, tecnologia"](#), Intervento all'Inaugurazione dell'Anno di Studi 2025-26 della Scuola di Polizia Economico-Finanziaria.

A queste iniziative possono dare un forte contributo la tecnologia e la ricerca, come testimonieranno gli interventi di oggi. La tecnologia può tuttavia agevolare anche i criminali, che infatti la utilizzano con abilità. Di seguito, dopo un accenno alle nuove tendenze della criminalità organizzata, mi soffermerò sul tema dell'utilizzo delle cripto-attività a fini illegali.

2. Nuove tendenze nel mondo della criminalità organizzata

L'integrazione e la mimetizzazione delle attività criminali nell'economia legale caratterizzano l'intera storia dell'illegalità. Il fenomeno non è agevole da misurare: dati affidabili per il confronto nel tempo, o tra paesi, non sembrano disponibili⁴. La globalizzazione si è accompagnata all'espansione transnazionale della criminalità. Più di recente, in concomitanza con il deteriorarsi delle relazioni internazionali, si sono registrate crescenti connessioni tra attività criminali e Stati.

Un secondo importante sviluppo riguarda l'utilizzo delle nuove tecnologie a fini illegali, non solo in ambito digitale. Si pensi alla continua immissione sul mercato di nuove droghe sintetiche, all'utilizzo della stampa 3D per la produzione di armi e a quello di droni per il traffico di droga⁵. Alcuni gruppi criminali sono impegnati nella frode informatica su scala industriale⁶. Una manifestazione di questa tendenza è quella delle frodi su pagamenti a danno della clientela bancaria. Tali frodi sono in aumento in Italia negli ultimi anni, anche se il loro valore risulta stabile in rapporto al totale delle transazioni. Si registrano casi recenti di aggiramento delle procedure di identificazione online della clientela utilizzate dalle banche attraverso il ricorso a immagini reali modificate, o completamente sintetiche.

Una ulteriore tendenza di rilievo riguarda la specializzazione delle attività illecite in base ai modelli del *crime-as-a-service* e del *fraud-as-a-service*, con la costituzione di reti internazionali, segmentate per attività e per macroarea geografica, che forniscono veri e propri servizi all'industria del crimine e delle frodi⁷.

Al contempo prosegue l'espansione dei mercati illegali. Si stima che i consumatori di sostanze psicotrope, che alimentano un mercato assai redditizio per le organizzazioni criminali, siano aumentati del 29 per cento tra il 2013 e il 2023⁸.

⁴ Secondo alcune fonti, nel 2024 i profitti della criminalità organizzata sarebbero stati pari al 5 per cento del PIL mondiale. Cfr. [The Millennium Project](#). Per evidenze sull'Italia, cfr. Comitato di Sicurezza Finanziaria, "[Analisi Nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo](#)", novembre 2024.

⁵ Cfr. G. Melillo, XIX Legislatura, "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 organised crime](#)"; P. Williams (2024), "[The fifth wave - Organized crime in 2040](#)", Global Initiative against Transnational Organized Crime.

⁶ Cfr. The Economist, "[The vast and sophisticated global enterprise that is Scam Inc](#)", 6 febbraio 2025 e Global Initiative against Transnational Organized Crime (2025), "[Compound crime - Cyber scam operations in Southeast Asia](#)".

⁷ Cfr. Europol (2013 e 2017), "[European Union Serious And Organised Crime Threat Assessment](#)".

⁸ Il dato si riferisce alla popolazione della fascia d'età tra i 15 e i 64 anni, che sarebbe passata da 246 milioni nel 2013 a 316 milioni nel 2023 (UNODC [World Drug Report](#), 2025, consultato il 31 ottobre).

3. Sviluppi nel mondo della finanza e dei pagamenti

Questo insieme di attività illegali crea una propria domanda di servizi finanziari e di pagamento, che beneficia della rivoluzione digitale nel sistema finanziario⁹. In questo ambito, un tema di grande interesse è quello dell'utilizzo delle cripto-attività a fini di riciclaggio e finanziamento del terrorismo. E' un fenomeno non nuovo, ma che sta registrando sviluppi che lo rendono di grande attualità sotto molteplici aspetti, compresi quelli AML/CFT.

Il contrasto all'utilizzo illecito delle cripto-attività avviene in primo luogo attraverso la regolamentazione degli intermediari specializzati, i quali gestiscono gran parte delle transazioni in cripto-attività. Questi intermediari, nati per custodire i bitcoin dei clienti e per consentirne la conversione in valuta legale e viceversa, nel tempo hanno esteso la propria offerta a centinaia di *token* e a più complessi servizi di negoziazione e investimento. Sotto la guida e l'impulso del Gruppo d'Azione Finanziaria Internazionale (GAFI), le principali giurisdizioni hanno regolamentato questi operatori. Nella UE, MiCAR ha introdotto la figura dei prestatori di servizi in cripto-attività (CASP nell'acronimo inglese), che devono sottostare a regole in materia AML/CFT non dissimili da quelle in vigore per gli intermediari finanziari tradizionali. Previsioni con finalità analoghe sono presenti in diversi Paesi, inclusi gli Stati Uniti.

Nel complesso, sebbene la regolamentazione sia ben lontana da una auspicabile armonizzazione a livello internazionale, il contrasto all'utilizzo delle cripto-attività a fini illegali attraverso la regolarizzazione degli intermediari del settore pare avviato.

Proprio in ragione dell'eterogeneità normativa rimane importante il ruolo degli intermediari tradizionali. Ad esempio, un utente europeo potrebbe tentare di eludere i controlli previsti da MiCAR operando in cripto-attività su piattaforme residenti in giurisdizioni più accomodanti. Non potrebbe però eludere i controlli messi in atto dagli istituti bancari nel momento in cui chiedesse alla piattaforma estera di convertire le cripto-attività in moneta legale e trasferire quest'ultima su un conto nella UE. In questo ambito, quindi, i meccanismi tradizionali del contrasto all'illegalità sono già attivi, e richiedono adattamenti concettualmente semplici, anche se magari complessi in pratica.

Sul piano AML/CFT le cripto-attività pongono tuttavia alcuni problemi specifici di non facile soluzione. Il più evidente è quello connesso con la possibilità di scambiare questi strumenti senza passare per gli intermediari specializzati. È noto che le cripto-attività sono nate proprio con l'obiettivo di fare a meno dell'intermediazione finanziaria e possono essere scambiate direttamente tra privati, tramite i cosiddetti portafogli elettronici auto-custoditi (*unhosted* o *self-custodial wallets*). Si tratta di combinazioni di software e hardware, facilmente reperibili, che consentono all'utente di custodire e utilizzare direttamente le proprie cripto-attività senza essere sottoposto ad 'adequata verifica'

⁹ F. Panetta, "[Moneta e fiducia, dal Rinascimento all'era digitale](#)", 2025; P. Cipollone, "Intervento di apertura alla conferenza ["The future of payments: CBDC, digital assets and digital capital markets"](#) organizzata dall'Università Bocconi, dal Centre for Economic Policy Research e dalla Banca centrale europea, 2025.

da parte di intermediari, operando quindi sulle *blockchain* in pseudo-anonimato¹⁰; si distinguono dai portafogli *hosted* (o *custodial*), che sono invece gestiti da un CASP e sono quindi sottoposti alla normativa AML/CFT¹¹.

Oggi, quindi, un criminale può sostituire la classica valigetta di banconote di grosso taglio con un portafoglio auto-custodito, una sorta di “valigetta elettronica” che non solo è in grado di contenere valori estremamente più elevati ma che può essere comodamente conservata e trasportata su un dispositivo simile a una chiavetta USB integrata con sistemi di crittografia avanzata, o su un cellulare.

In questo contesto assume rilievo il fenomeno delle *stablecoin*: cripto-attività generalmente riconducibili a un emittente che mantengono un valore ancorato a una o più attività, tipicamente una valuta ufficiale, e consentono dunque ai criminali di minimizzare il rischio connesso con l’elevata volatilità del valore di certe altre cripto-attività (ad esempio Bitcoin). La “valigetta elettronica” può dunque contenere importi monetari non solo elevatissimi, ma anche di valore sostanzialmente stabile. Le *stablecoin* rappresentano quindi un “rischio rosso” per il sistema di contrasto al riciclaggio e alla criminalità organizzata.

Il contrasto all’utilizzo illegale dei portafogli auto-custoditi è a uno stadio preliminare. La normativa europea prevede che i CASP, qualora i propri clienti interagiscano con portafogli auto-custoditi, adottino misure per verificare l’identità degli utilizzatori di questi ultimi¹². Da interlocuzioni preliminari tra la Vigilanza e i CASP italiani emerge che essi starebbero adottando misure di mitigazione dei rischi derivanti dall’uso di questi strumenti, tra cui meccanismi basati su *whitelist* di portafogli autorizzati, nonché strumenti di analisi in grado di esaminare i registri pubblici delle *blockchain*. Questi strumenti aiutano a portare alla luce transazioni sospette (ad esempio quelle legate a gruppi criminali informatici, entità sanzionate e operatori o soggetti in giurisdizioni a rischio).

Una seconda modalità di contrasto all’utilizzo illegale dei portafogli auto-custoditi coinvolge direttamente gli emittenti di cripto-attività. Questi ultimi possono non solo monitorare le transazioni quando sono registrate su *blockchain* pubbliche (similmente ai CASP, o alle forze dell’ordine, o a qualunque altro soggetto dotato di adeguate capacità tecniche); sotto certe condizioni, possono anche riuscire a bloccare o recuperare cripto-attività utilizzate in attività sospette o illecite, anche se detenute in portafogli auto-custoditi¹³. Sarebbe

¹⁰ Le transazioni registrate sulle *blockchain* pubbliche sono liberamente consultabili, ma coinvolgono i cosiddetti “indirizzi virtuali”, stringhe alfanumeriche casuali che non contengono informazioni utili a risalire direttamente all’identità e alla localizzazione dei loro utilizzatori. Tuttavia, in alcuni casi è possibile, analizzando le transazioni, individuare gli indirizzi potenzialmente controllati dalla medesima entità (c.d. “*clustering*”) e de-anonimizzarli nei casi in cui siano disponibili ulteriori informazioni utili a collegarli a identità reali (ad es. per il *listing* da parte di autorità o la condivisione di un indirizzo su un profilo *social*).

¹¹ I portafogli auto-custoditi, quindi, a fronte di maggiori rischi (ad esempio, perdita delle chiavi che consentono di sbloccare le cripto-attività detenute, furto o danneggiamento dell’hardware), garantiscono agli utilizzatori, come detto, più elevati livelli di anonimato nonché maggiore autonomia nella gestione e – talvolta – costi inferiori di utilizzo.

¹² Cfr. il Regolamento (UE) 2023/1113, Transfer of Funds Regulation (TFR).

¹³ Ciò presuppone che l’emittente abbia previsto tale possibilità negli *smart contract* che governano l’emissione e la circolazione di un token. A tali fini non sarebbe richiesta la conoscenza delle chiavi private dei portafogli auto-custoditi, necessarie invece per il sequestro delle cripto-attività prive di un emittente (come il Bitcoin).

quindi auspicabile che agli obblighi previsti per i prestatori di servizi in cripto-attività si affiancassero previsioni chiare volte a disciplinare questi poteri degli emittenti. Previsioni del genere non sono presenti nella legislazione attuale della UE, mentre iniziano ad essere introdotte o sono in discussione in altre giurisdizioni, ad esempio negli Stati Uniti¹⁴.

Rimane il fatto che transazioni effettuate esclusivamente mediante portafogli auto-custoditi senza passare dalla *blockchain* sfuggono al controllo sia degli emittenti sia degli operatori specializzati¹⁵. Si assiste inoltre alla diffusione, ancora limitata in ambito europeo, di schemi di finanza decentralizzata (c.d. "DeFi"), nei quali servizi in cripto-attività sono svolti in assenza di CASP e quindi senza i presidi AML/CFT¹⁶.

Oggi pressoché l'intero ammontare di stablecoin in circolazione è denominato in dollari statunitensi e fa capo a due emittenti, Tether International S.A. e Circle. Tether ha sede legale in El Salvador e non è autorizzata ai sensi delle regolamentazioni europea e statunitense¹⁷. In Europa le stablecoin emesse da Tether non possono essere negoziate da CASP, e i loro scambi sono soggetti a presidi AML/CFT limitati in ambito UE¹⁸; questi ultimi si applicano invece alle transazioni in stablecoin emesse da Circle¹⁹ (che rispetta i requisiti di MiCAR), ma solo quando esse avvengono tramite CASP.

Attualmente lo stock di stablecoin in circolazione ha un controvalore di circa 310 miliardi di dollari, un importo rilevante in valore assoluto ma del tutto trascurabile se rapportato ad esempio alla consistenza dei depositi bancari negli Stati Uniti (1,5 per cento)²⁰. Il vivace dibattito in corso a livello internazionale sui rischi delle stablecoin è motivato dai

¹⁴ Il *Genius Act* contiene riferimenti alla disciplina AML/CFT applicabile nei confronti degli emittenti autorizzati di *stablecoin*; in tale ambito sono ad esempio menzionate "*technical capabilities, policies, and procedures to block, freeze, and reject specific or impermissible transactions that violate Federal or State laws, rules, or regulations*". Nel Regno Unito un [documento di consultazione](#) appena pubblicato dalla Banca d'Inghilterra sulla regolamentazione delle *stablecoin* con rilevanza sistemica prevede l'applicazione degli obblighi AML/CFT nell'ambito del processo di rimborso dei token; obblighi AML/CFT in capo agli emittenti delle altre *stablecoin* sono stati proposti a maggio 2025 dalla [Financial Conduct Authority](#), competente in materia.

¹⁵ Si tratta di transazioni effettuate mediante cessione della chiave crittografica privata, senza trascrizione sulla *blockchain*.

¹⁶ Cfr. ESMA ed EBA, "[Recent developments in crypto-assets \(Article 142 of MiCAR\)](#)".

¹⁷ Secondo le [valutazioni ufficiali del GAFILAT](#), organismo regionale del GAFI, il sistema AML/CTF di El Salvador ha evidenziato nel 2024 progressi ma rimane caratterizzato da significative criticità, in particolare sul fronte della supervisione.

¹⁸ Come evidenziato dall'[ESMA](#), i CASP non possono offrire al pubblico o negoziare cripto-attività (ART o EMT) che non rispettano i requisiti previsti da MiCAR; tuttavia possono gestire il trasferimento di tali attività da/a terzi e la relativa custodia, e quindi su questi servizi sono applicabili i presidi AML/CFT.

¹⁹ USDC è emesso secondo uno schema "multi-emittente" dalla società statunitense Circle Internet Financial LLC e dalla francese Circle Internet Financial Europe SAS, utilizzando la medesima denominazione commerciale. Quest'ultima è soggetta a MiCAR e alla vigilanza dell'ACPR.

²⁰ In base alle informazioni disponibili, queste *stablecoin* vengono utilizzate prevalentemente per transazioni in altre cripto-attività. Gli utilizzi a fini illeciti sono ricompresi in questo ambito, anche se presumibilmente non lo esauriscono. Si registra inoltre un utilizzo delle *stablecoin* in paesi caratterizzati da instabilità monetaria, dove è relativamente forte la domanda di attività non soggette a perdita di valore. Vi è infine evidenza aneddotica di un terzo utilizzo, a fini di rimesse da parte degli emigrati. Cfr. ad es. R. Auer, U. Lewrick and J. Paulick (2025), "[DeFying Gravity? An Empirical Analysis of Cross-Border Bitcoin, Ether and Stablecoin Flows](#)", BIS Working Papers n. 1265; I. Alsadoro, M. Aquilina, U. Lewrick e S.H. Lim (2025), "[Stablecoin growth – policy challenges and approaches](#)", BIS Bulletin n. 108.

timori per le conseguenze connesse con il loro potenziale di crescita. Stablecoin ancorate all'euro che venissero distribuite da grandi gruppi tecnologici, che hanno accesso a enormi basi di clienti, potrebbero rapidamente acquisire un'accettabilità non lontana da quella degli strumenti di pagamento tradizionali. Qualora ciò accadesse potrebbe attenuarsi, o addirittura venire meno, l'esigenza di convertire i flussi di origine criminale in strumenti tradizionali. Alla luce di quanto detto sopra, sono evidenti le difficoltà che si creerebbero per il contrasto alle attività illegali. Si porrebbero inoltre rischi per la stabilità finanziaria, su cui non mi soffermo²¹.

Il *Virtual asset contact group* del GAFI è impegnato nell'analisi e nella mitigazione dei rischi AML/CFT legati alle stablecoin e alla finanza decentralizzata²²; su questi temi saranno pubblicati rapporti specifici, che potranno essere da stimolo per accrescere l'efficacia dei presidi di prevenzione e mitigare i rischi di arbitraggi normativi.

4. Conclusioni

I progressi della tecnologia vengono sfruttati sia dall'industria criminale sia dal sistema incaricato del suo contrasto. La Banca d'Italia, e la UIF in particolare, dispongono di un vasto patrimonio informativo, in buona parte unico a livello internazionale, che consente di modellare comportamenti, individuare aree di rischio, valutare la portata della infiltrazione criminale nei diversi settori, considerando non solo gli interessi economici, ma anche la dimensione relazionale della fenomenologia criminale. Alcuni risultati di questa attività saranno illustrati nel corso della giornata.

Da questi lavori emerge che i metodi quantitativi, associati a microdati di alta qualità, possono incrementare significativamente l'efficienza e l'efficacia dell'azione dell'UIF, facendo fronte all'aumentata raffinatezza e complessità delle tecniche utilizzate dalle organizzazioni criminali per eludere i controlli.

Il buon funzionamento del sistema di contrasto all'illegalità richiede la condivisione di tecniche, informazioni e risultati – e più in generale l'interazione strategica e la cooperazione – tra tutti gli attori del sistema: autorità di controllo, organi investigativi, autorità giudiziaria, industria degli intermediari, mondo della ricerca. L'iniziativa odierna ha questo obiettivo; testimonia l'impegno delle nostre istituzioni e delle nostre aziende per la tutela della legalità del sistema economico.

²¹ Nel dibattito corrente si sottolineano i rischi di corse ai rimborsi e quelli insiti negli schemi che emettono uno stesso strumento attraverso emittenti con sede legale in paesi diversi; cfr. ad esempio Financial Stability Board, [“FSB Plenary sets out 2026 work plan”](#), 2025; Banca d'Italia, [Rapporto sulla stabilità finanziaria](#), n. 2, 2025.

²² Cfr. FATF, [“Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers”](#), giugno 2025.

