SCUOLA SUPERIORE DELLA MAGISTRATURA

Formazione Decentrata della Corte d'Appello di Lecce
Corso D26205 — 15 aprile 2026 | ore 15.30-18.30
Aula Magna, Corte d'Appello di Lecce

CRIPTO-ATTIVITÀ NEL SISTEMA GIURIDICO:
Repressione penale, tutela patrimoniale, prevenzione AML e prova digitale

RELAZIONE FORMATIVA

Dalla nascita di Bitcoin agli scenari giudiziari contemporanei

Dr. Luigi Patruno | Funzionario bancario, Esperto Tecnico Finanziario e AML
Dr. Silverio Greco | Consulente Tecnico Informatico Forense
Magistrato Formatore: Dott. Antonio Ivan Natali

Pubblicazione riservata ai partecipanti e agli iscritti al sito SSM. Riproduzione consentita con citazione della fonte.

ABSTRACT

La presente relazione costituisce il documento formativo ufficiale del Corso D26205 della Scuola Superiore della Magistratura, tenutosi il 15 aprile 2026 presso l'Aula Magna della Corte d'Appello di Lecce nell'ambito della Formazione Decentrata. Il corso, della durata di tre ore, è stato articolato in cinque moduli tematici ed ha coinvolto magistrati ordinari e onorari — GOT, GOP, VPO, Giudici di Pace — in funzione e in tirocinio, con particolare destinazione ai magistrati di prima nomina (MOT) chiamati a esercitare funzioni sia civili sia penali.

Il fenomeno delle cripto-attività ha assunto negli ultimi anni dimensioni tali da rendere indifferibile una formazione specialistica della magistratura italiana. I dati più recenti documentano sequestri di asset digitali per un valore complessivo di circa 18 miliardi di euro in Europa nel biennio 2022-2024, un aumento del 340% dei procedimenti penali che coinvolgono cripto-attività nei tribunali italiani, e l'entrata in vigore del primo quadro regolatorio organico a livello globale — il Regolamento UE 2023/1114 (MiCA) — che ridisegna l'intero settore a partire dal 2024.

La relazione affronta in modo sistematico e con taglio operativo il fenomeno delle cripto-attività nei suoi molteplici risvolti giuridici, coprendo: i profili tecnico-definitòri e la genesi storica del fenomeno; le principali fattispecie penali connesse, con analisi della giurisprudenza più recente in materia di sequestro, confisca e riciclaggio; i profili civilistici e patrimoniali rilevanti in sede di separazione, successione e tutela del creditore; il sistema di prevenzione antiriciclaggio con le novità introdotte da MiCA e dalla Travel Rule europea; e le tecniche di acquisizione della prova digitale e di tracciamento blockchain nelle indagini giudiziarie.

L'impostazione metodologica privilegia il caso pratico e l'applicazione diretta degli strumenti giuridici disponibili, a partire dalla giurisprudenza di legittimità — in primo luogo Cass. pen. Sez. II n. 26807/2021 sulla qualificazione del Bitcoin come cosa mobile — e dalla normativa di riferimento, con particolare attenzione alle novità del 2024-2025 che non sono ancora entrate nella manualistica tradizionale.

INDICE

CAPITOLO I — Il Contesto: Perché la Magistratura Deve Conoscere le Cripto-Attività

1.1 Dimensioni del fenomeno

Il fenomeno delle cripto-attività non è più una questione di nicchia tecnologica o finanziaria. È già dentro i fascicoli processuali italiani, quotidianamente, in forme che sfidano la preparazione tradizionale del giurista. Tre dati fotografano la dimensione del problema con chiarezza inequivocabile.

Il primo dato riguarda il valore degli asset sequestrati: circa 18 miliardi di euro in Europa nel biennio 2022-2024, con un incremento esponenziale rispetto ai periodi precedenti. Il secondo dato riguarda la crescita dei procedimenti: un aumento del 340% dei fascicoli che coinvolgono cripto-attività nei tribunali italiani nell'ultimo triennio. Il terzo dato è normativo: l'entrata in vigore del Regolamento MiCA nel 2024 ha creato per la prima volta un quadro di riferimento organico, ma ha anche generato nuove figure di illecito e nuovi obblighi di vigilanza che il magistrato deve conoscere.

La Corte di Cassazione ha già sciolto alcuni nodi fondamentali — la qualificazione del Bitcoin come cosa mobile, la sufficienza del dolo eventuale per il riciclaggio, la configurabilità dello swap tra crypto come condotta di sostituzione. Ma molte questioni rimangono aperte, e ogni sentenza emessa oggi contribuisce a costruire un diritto che non è ancora scritto nei libri.

1.2 La genesi storica: trent'anni prima di Bitcoin

Per comprendere le cripto-attività e interpretare correttamente i comportamenti degli autori di reato, è indispensabile conoscere la genesi storica del fenomeno. Le criptovalute non sono nate come strumento criminale. Sono nate come strumento politico — come risposta ideologica a quello che i suoi creatori percepivano come un sistema finanziario centralizzato, opaco e intrinsecamente ingiusto.

Il movimento Cypherpunk, attivo dalla fine degli anni Ottanta, costituisce il terreno ideologico da cui nasce Bitcoin. Il termine, che unisce 'cipher' (cifratura) e 'punk' (attitudine ribelle), identifica un gruppo di informatici, matematici e crittografi americani che perseguivano l'obiettivo di costruire sistemi di comunicazione e di scambio economico sottratti al controllo governativo. Il loro manifesto, redatto da Eric Hughes nel marzo 1993, proclamava: 'La privacy è necessaria per una società aperta nell'era elettronica. Non possiamo aspettarci dai governi che ce la concedano. Dobbiamo difenderla noi stessi.'

> *«La privacy è necessaria per una società aperta nell'era elettronica. Non possiamo aspettarci dai governi, dalle aziende o da altre grandi organizzazioni senza volto che ci concedano la privacy. Dobbiamo difenderla noi stessi.» — Eric Hughes, A Cypherpunk's Manifesto, 9 marzo 1993*

Prima di Bitcoin, tra il 1990 e il 2007, i Cypherpunk tentarono almeno cinque volte di creare una moneta digitale decentralizzata. DigiCash di David Chaum (1990) fallì perché nessuna banca volle adottarla. Hashcash di Adam Back (1997) introdusse il concetto di proof of work — che Satoshi Nakamoto avrebbe ripreso pari pari — ma non risolse il problema del double spending. B-money di Wei Dai (1998) propose per la prima volta una moneta decentralizzata. Bit Gold di Nick Szabo (stesso anno) era strutturalmente identico a Bitcoin, al punto che Szabo rimane oggi il candidato più credibile per essere Satoshi Nakamoto. Tutti questi progetti fallirono per lo stesso motivo: non riuscivano a impedire che la stessa moneta venisse spesa due volte senza affidarsi a un'autorità centrale.

La crisi finanziaria del 2008 — il fallimento di Lehman Brothers il 15 settembre, il salvataggio pubblico delle banche con il denaro dei contribuenti — fornì il catalizzatore politico e il contesto ideale per il lancio di Bitcoin. Non fu una coincidenza: fu una scelta deliberata e simbolicamente potente.

1.3 Il 31 ottobre 2008 e il Blocco Genesi

Il 31 ottobre 2008, alle 18:10 ora italiana, un'entità pseudonima denominata Satoshi Nakamoto invia un'email a una mailing list di crittografi con oggetto 'Bitcoin P2P e-cash paper'. Il messaggio introduce il White Paper di Bitcoin — nove pagine che descrivono un sistema di pagamento elettronico completamente peer-to-peer, senza terze parti di fiducia.

Il 3 gennaio 2009, alle 18:15 UTC, viene minato il primo blocco della blockchain Bitcoin — il cosiddetto Blocco Genesi o Genesis Block. Nel codice del blocco, Satoshi Nakamoto incide per sempre una frase: 'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks'. Era il titolo del quotidiano britannico The Times di quel giorno, che annunciava l'intenzione del ministro delle finanze del Regno Unito di destinare ulteriori fondi pubblici al salvataggio del sistema bancario. Non si trattava di un dettaglio tecnico: era una dichiarazione politica, incisa in modo irreversibile nel primo blocco di una blockchain che, finché esisterà internet, sarà accessibile a chiunque nel mondo.

> *«The Times 03/Jan/2009 Chancellor on brink of second bailout for banks» — Satoshi Nakamoto, Genesis Block, 3 gennaio 2009*

Nove giorni dopo il lancio della rete, Hal Finney — crittografo californiano, figura di spicco del movimento Cypherpunk — ricevette la prima transazione Bitcoin della storia: dieci Bitcoin da Satoshi Nakamoto stesso. Finney morì nel 2014, affetto da SLA, senza rivelare l'identità di Satoshi. L'ipotesi che fosse egli stesso Satoshi rimane la più accreditata tra i ricercatori.

Satoshi Nakamoto rimase attivo nello sviluppo del protocollo fino all'aprile 2011, quando consegnò le chiavi di amministrazione della rete allo sviluppatore Gavin Andresen e scomparve. Il suo wallet, che contiene circa un milione di Bitcoin pari a oltre 80 miliardi di euro al valore corrente, non è mai stato toccato. Per il magistrato, questa circostanza non è solo una curiosità: quel wallet rappresenta la più grande potenziale controversia successoria della storia del diritto privato.

CAPITOLO II — Fondamenta Tecnologiche: Cosa il Magistrato Deve Sapere

2.1 Definizione normativa e tassonomia MiCA

Il Regolamento UE 2023/1114 (MiCA — Markets in Crypto-Assets), in vigore dal 2024, fornisce la prima definizione legale organica a livello europeo. L'articolo 3 definisce le cripto-attività come 'rappresentazione digitale di un valore o di un diritto che può essere trasferita e conservata elettronicamente utilizzando la tecnologia a registro distribuito o una tecnologia analoga'.

MiCA distingue quattro categorie, ciascuna soggetta a un regime diverso con implicazioni dirette per la qualificazione giuridica e il regime sanzionatorio applicabile.

Criptovalute (es. Bitcoin, Ethereum)

Prive di emittente identificabile, con offerta algoritmicamente definita. Bitcoin ed Ethereum sono esclusi dall'ambito di applicazione di MiCA in quanto già diffusi e decentralizzati. Non hanno garanzie statali, non sono moneta legale, ma sono riconosciuti come beni mobili dalla giurisprudenza italiana.

Token Referenziati ad Attività (ART — Asset-Referenced Tokens)

Cripto-attività che mantengono un valore stabile con riferimento a valute fiat, materie prime o panieri di asset. Esempio: USDT agganciato al dollaro USA, PAXG agganciato all'oro. Soggetti a MiCA Titolo III con obbligo di autorizzazione CONSOB/Banca d'Italia.

Token di Moneta Elettronica (EMT — E-Money Tokens)

Cripto-attività riferite a una singola valuta fiat con diritto di rimborso al portatore. Equiparati agli istituti di moneta elettronica. Soggetti a MiCA Titolo IV e alla disciplina degli IMEL.

Altre cripto-attività: Utility Token, Security Token, NFT

Gli Utility Token danno accesso a servizi sulla piattaforma emittente e sono esclusi da MiCA se non hanno natura finanziaria. I Security Token rappresentano strumenti finanziari e ricadono sotto MiFID II e TUF. Gli NFT — Non-Fungible Token — sono beni digitali unici e non intercambiabili, con rilevanza crescente in materia di diritto d'autore, contraffazione, e — come vedremo — riciclaggio.

> Nota operativa per il magistrato: la categoria determina il regime applicabile e la tutela disponibile per le vittime. La prima domanda da porsi di fronte a un fascicolo che coinvolge cripto non è 'quanto vale?' ma 'di quale categoria si tratta?'. Da quella risposta dipende chi vigila, quali obblighi si applicano e se esistono garanzie per l'investitore danneggiato.

2.2 Come funziona la blockchain: il registro immutabile

La blockchain è un registro distribuito — un database che non risiede su un server centrale ma è replicato simultaneamente su migliaia o milioni di computer nel mondo. Ogni partecipante alla rete ne detiene una copia identica e aggiornata in tempo reale. L'assenza di un centro di controllo è la caratteristica fondante: non esiste un'autorità che possa modificare retroattivamente i dati registrati.

Il processo di registrazione di una transazione si articola in cinque fasi. Prima fase: l'utente A firma la transazione con la propria chiave privata — una firma crittografica che garantisce l'autenticità e l'autorizzazione senza rivelare l'identità dell'autore. Seconda fase: la transazione viene trasmessa a tutta la rete e inserita in una coda di attesa denominata mempool. Terza fase: i miner — computer specializzati — raccolgono le transazioni in attesa e le raggruppano in un blocco. Quarta fase: il blocco viene validato attraverso il meccanismo di consenso: Proof of Work per Bitcoin, Proof of Stake per Ethereum. Quinta fase: il blocco validato viene aggiunto alla catena — da quel momento la transazione è permanente, immutabile e definitiva.

Ogni blocco contiene l'impronta digitale crittografica — l'hash — del blocco precedente. Questa concatenazione garantisce l'immutabilità: modificare un blocco passato richiederebbe di ricalcolare l'hash di tutti i blocchi successivi e di farlo più velocemente di tutti i computer del mondo messi insieme. È computazionalmente impossibile.

> Per il magistrato, l'immutabilità della blockchain non è una promessa commerciale: è una certezza matematica. Una transazione registrata sulla blockchain è avvenuta. È datata con precisione al secondo. È collegata a un indirizzo. Non può essere cancellata retroattivamente da nessuno — nemmeno dal creatore del protocollo. Questo la rende la fonte probatoria più affidabile e permanente che esista per i flussi di valore digitale.

2.3 Wallet, chiavi e seed phrase: il controllo degli asset

Il wallet — portafoglio digitale — non contiene Bitcoin nel senso fisico del termine. Contiene le chiavi crittografiche che permettono di accedere agli asset registrati sulla blockchain. La distinzione è cruciale per comprendere le implicazioni processuali.

La chiave pubblica è analoga all'IBAN: chiunque può usarla per inviare fondi all'indirizzo corrispondente. La chiave privata è analoga alla password del conto corrente: chi la possiede può disporre dei fondi. Perdere la chiave privata significa perdere i fondi per sempre — non esiste un numero verde, non esiste una filiale dove recarsi. La seed phrase — una sequenza di 12 o 24 parole in inglese generata alla creazione del wallet — è il backup della chiave privata: chiunque la conosca può accedere a tutti i fondi.

I wallet si distinguono in tre categorie con rilevanza processuale diretta. Il hot wallet è un'applicazione su smartphone o computer connessa a internet: comoda ma vulnerabile ad attacchi informatici. Il cold wallet è un dispositivo fisico offline — simile a una chiavetta USB specializzata — estremamente sicuro: va sequestrato fisicamente in perquisizione. Il wallet custodial presso un exchange è quello in cui l'exchange detiene le chiavi per conto dell'utente: tecnicamente è un credito verso l'exchange, sequestrabile con ordine diretto al VASP. Il wallet non-custodial in ambiente DeFi è il più difficile da aggredire: l'utente controlla tutto, non esiste un intermediario.

> Il tipo di wallet determina la strategia processuale. Custodial presso exchange noto: ordine diretto al VASP. Hardware wallet trovato fisicamente: perizia tecnica sul device. Wallet non-custodial con chiavi non disponibili: confisca per equivalente su altri beni. Queste tre strade hanno esiti completamente diversi.

2.4 Cripto-attività e moneta legale: differenze con implicazioni giuridiche dirette

La distinzione tra cripto-attività e moneta legale non è solo tecnica: ha conseguenze dirette in ogni ramo del diritto.

Le cripto-attività non sono moneta legale. L'articolo 128 del TFUE impone a tutti di accettare l'euro come mezzo di pagamento nei territori dell'Unione. Le cripto-attività non hanno corso legale: nessuno è obbligato ad accettarle. Un commerciante può legittimamente rifiutarle. Un'obbligazione pecuniaria si adempie in euro salvo accordo contrario esplicito.

L'irreversibilità della transazione è la caratteristica che più distingue le cripto dalla moneta bancaria. Una transazione confermata sulla blockchain è definitiva: non si storna, non si annulla, non si recupera. Se un acquirente ha pagato e il venditore non consegna il bene, la blockchain non rimborsa. Questa caratteristica impatta direttamente sulla tutela del consumatore, sulla possibilità di recuperare i proventi illeciti, e sulla quantificazione del danno.

La volatilità estrema ha implicazioni processuali rilevanti. Bitcoin ha perso il 70% del valore in pochi mesi nel 2022 per poi tornare ai massimi nel 2024. Questo significa che la data di cristallizzazione del valore è cruciale: il profitto illecito da quantificare, il patrimonio da dividere in sede di separazione, il cespite da liquidare nel fallimento possono differire enormemente a seconda della data di riferimento scelta.

Sul limite di emissione: non potranno mai esistere più di 21 milioni di Bitcoin. Scritto nel codice del protocollo nel 2008, questo limite è matematicamente irreversibile. Ogni circa quattro anni la ricompensa per i miner si dimezza — si chiama halving. Nel 2009 era 50 Bitcoin per blocco; oggi

è 3,125. Il 93% di tutti i Bitcoin è già stato creato. Si stima che circa 3-6 milioni di Bitcoin — tra 250 e 500 miliardi di euro — siano definitivamente persi perché i proprietari sono deceduti senza trasmettere le chiavi o le hanno smarrite.

CAPITOLO III — Il Sistema Penale: Reati, Sequestro e Confisca

3.1 Mappa delle fattispecie penali

Le fattispecie penali connesse alle cripto-attività si articolano in tre grandi famiglie, ciascuna con caratteristiche investigative e processuali proprie.

3.1.1 Reati economico-finanziari

Il riciclaggio ex articolo 648-bis del codice penale è la fattispecie di gran lunga più frequente. Le cripto-attività sono diventate lo strumento preferito per il reimpiego dei proventi illeciti per ragioni che, paradossalmente, ne facilitano anche il tracciamento. L'autoriciclaggio ex articolo 648-ter.1, introdotto dalla legge 186 del 2014, si configura quando il medesimo soggetto che ha commesso il reato presupposto reimpega i proventi.

L'abusivismo finanziario ex articolo 166 TUF si configura quando un VASP offre servizi di investimento senza la prescritta autorizzazione. Con l'entrata in vigore di MiCA e del D.Lgs. 129/2024, chi opera come Crypto Asset Service Provider senza autorizzazione è perseguibile anche per l'illecito amministrativo ex articolo 17-bis D.Lgs. 231/2007 (sanzione fino a 700.000 euro), oltre che penalmente.

La manipolazione di mercato ex articolo 187-ter TUF e l'insider trading ex articolo 184 TUF sono ora applicabili alle cripto-attività classificate come strumenti finanziari, con l'ulteriore supporto dell'articolo 92 del Regolamento MiCA per le fattispecie di market abuse nell'ambito delle cripto-attività non finanziarie.

3.1.2 Reati informatici

La frode informatica ex articolo 640-ter del codice penale — mediante alterazione di sistemi o intercettazione di credenziali — è frequente nei casi di furto di wallet o compromissione di exchange. L'accesso abusivo ex articolo 615-ter è contestato sistematicamente nei casi di ransomware e nei furti di cripto da piattaforme. Il danneggiamento informatico ex articolo 635-bis si configura nei casi di cifratura dei dati della vittima in cambio di riscatto in cripto.

Il ransomware merita una trattazione specifica per la sua crescente diffusione. Lo schema tipico prevede: intrusione nei sistemi della vittima (615-ter), cifratura dei dati (635-bis), richiesta di riscatto in Bitcoin o Monero (629), possibile riciclaggio del riscatto (648-bis). La questione processuale più controversa — ancora aperta — riguarda la configurabilità del finanziamento al crimine in capo alla vittima che decide di pagare il riscatto.

3.1.3 Crimine organizzato

L'associazione mafiosa ex articolo 416-bis e l'associazione per delinquere ex articolo 416 trovano applicazione quando le cripto-attività costituiscono il patrimonio illecito dell'organizzazione da reinvestire. I marketplace del darknet su reti TOR, con pagamento in Bitcoin o Monero, sono lo strumento principale per il traffico di stupefacenti ex DPR 309/1990 articolo 73. Il finanziamento del terrorismo ex articolo 270-quinquies.2 del codice penale ha visto casi documentati di raccolta fondi in cripto-attività da parte di organizzazioni terroristiche.

3.2 Il sequestro preventivo: leading case e prassi operativa

Il sequestro preventivo delle cripto-attività ex articolo 321 del codice di procedura penale è stato oggetto di elaborazione giurisprudenziale significativa negli ultimi anni. Il leading case che ha risolto la questione della qualificazione giuridica è la sentenza della Cassazione penale, Sezione II, del 25 giugno 2021, numero 26807.

> *«Il Bitcoin, avendo un valore di scambio riconosciuto, è qualificabile come cosa mobile ai sensi dell'art. 624 c.p. e pertanto suscettibile di sequestro preventivo ex art. 321 c.p.p. Il periculum in mora può rinvenirsi nel rischio di dispersione del valore attraverso transazioni blockchain non reversibili.» — Cass. pen. Sez. II, 25 giugno 2021, n. 26807*

I presupposti del sequestro rimangono quelli ordinari: fumus commissi delicti — per qualsiasi reato per cui possa disporsi confisca — e periculum in mora. Quest'ultimo, nel caso delle cripto-attività, presenta caratteristiche peculiari: la transazione blockchain è istantanea, irreversibile, e non richiede intermediari. In pochi secondi, un indagato può trasferire qualsiasi importo in qualsiasi parte del mondo. Il rischio di dispersione è pertanto reale e immediato in misura superiore a qualsiasi altro asset tradizionale.

3.2.1 Modalità esecutive

Le modalità esecutive variano significativamente a seconda del tipo di wallet. Per i wallet custodial presso exchange registrati: ordine diretto al VASP per il blocco dell'account, per analogia con il pignoramento presso terzi. Per i device fisici — hardware wallet, smartphone con wallet installato —: sequestro fisico in perquisizione e successiva perizia tecnica. Per i wallet non-custodial: in assenza di collaborazione dell'indagato, il sequestro diretto è impossibile. Si ricorre alla confisca per equivalente su altri beni.

La nomina del custode giudiziario ex articolo 259 del codice di procedura penale presenta difficoltà pratiche non ancora risolte in modo uniforme. Il custode deve essere in grado di proteggere la chiave privata, gestire la cold storage, garantire la sicurezza informatica del seed. Non esiste un albo di custodi con competenze crittografiche. La soluzione più diffusa, adottata tra gli altri dal Tribunale di Milano con ordinanza del 2022, prevede la nomina di un perito informatico forense come custode con disposizione di conversione immediata del valore in euro al momento del sequestro — per cristallizzare il valore ed evitare responsabilità da volatilità.

3.2.2 VASP estero e cooperazione internazionale

Quando il wallet è custodial presso un exchange con sede in altro Stato, gli strumenti di cooperazione internazionale sono fondamentali. Per i paesi dell'Unione Europea: Ordine Europeo di Indagine ex D.Lgs. 108/2017 — tempi mediamente di 45-90 giorni. Per gli Stati Uniti e il Regno Unito: Mutual Legal Assistance Treaty (MLAT). Per i paesi non cooperativi: canale informale tramite la rete Egmont della UIF, che consente scambio di intelligence finanziaria tra le Financial Intelligence Unit di 170 paesi in 24-72 ore senza i formalismi della rogatoria.

3.3 La confisca: tipologie e questioni operative

Il sistema della confisca si articola in quattro strumenti con requisiti e ambiti di applicazione distinti.

La confisca facoltativa ex articolo 240 primo comma del codice penale — discrezionale, per il prodotto, il prezzo e il profitto del reato. La difesa può opporsi dimostrando la buona fede o l'interesse di terzi. La confisca obbligatoria ex articolo 240 secondo comma — automatica, per il prezzo del reato, senza possibilità di opposizione. La confisca per sproporzione ex articolo 240-bis — lo strumento più penetrante per i reati più gravi (mafia, traffico droga, corruzione): si confiscano tutti i beni di valore sproporzionato rispetto al reddito dichiarato, con inversione dell'onere probatorio. Il valore delle cripto-attività rientra nel calcolo della sproporzione. La confisca per equivalente ex articolo 322-ter — fondamentale quando il wallet è inaccessibile: si

confiscano beni di uguale valore. Garantisce l'effettività della risposta penale anche quando la seed phrase è nascosta o distrutta.

> Punto operativo cruciale: l'indagato che nasconde la seed phrase non la fa franca. La confisca per equivalente consente di aggredire immobili, conti correnti, veicoli per un valore pari agli asset digitali non accessibili. Questo strumento deve essere richiesto sistematicamente ogni volta che il wallet non è accessibile.

3.4 Il riciclaggio con cripto: anatomia del reato e prova dell'elemento soggettivo

Il riciclaggio ex articolo 648-bis del codice penale — nella sua applicazione alle cripto-attività — presenta alcune specificità che meritano attenzione.

3.4.1 La condotta

La condotta tipica comprende la sostituzione, il trasferimento e le 'altre operazioni'. La Cassazione penale, Sezione II, con sentenza numero 34895 del 2022, ha chiarito che anche lo swap tra cripto-attività diverse — ad esempio da Bitcoin a Monero — integra la condotta di sostituzione. Non è quindi necessario uscire dal mondo cripto per commettere riciclaggio: il semplice spostamento da una cripto all'altra, se finalizzato a ostacolare l'identificazione della provenienza illecita, è sufficiente.

> *«La conversione di Bitcoin in altra valuta virtuale integra la condotta di sostituzione prevista dall'art. 648-bis c.p., anche quando l'operazione avvenga all'interno del medesimo sistema blockchain.» — Cass. pen. Sez. II, n. 34895/2022*

Il reato presupposto: qualsiasi delitto non colposo. Non è richiesta la condanna definitiva — è sufficiente che il PM dimostri la provenienza delittuosa degli asset. Con il D.Lgs. 195/2021 di recepimento della VI Direttiva AML, anche i reati fiscali sono stati inclusi tra i reati presupposto.

3.4.2 L'elemento soggettivo: il dolo eventuale

La questione più dibattuta riguarda l'elemento soggettivo. La Cassazione penale, Sezione II, con sentenza numero 23017 del 14 giugno 2021, ha stabilito che il dolo eventuale è sufficiente: è necessario e sufficiente che il soggetto si sia rappresentato la possibilità che i fondi provenissero da un reato e abbia accettato questo rischio.

> *«Ai fini della configurabilità del delitto di riciclaggio, il dolo eventuale è sufficiente: è necessario che il soggetto si sia rappresentato la possibilità che il denaro o le altre utilità provengano da un'attività delittuosa e che abbia accettato tale rischio.» — Cass. pen. Sez. II, 14 giugno 2021, n. 23017*

Come si dimostra il dolo eventuale? Attraverso gli indici sintomatici che la giurisprudenza ha identificato: l'uso di mixer o tumbler per spezzare il collegamento blockchain; l'utilizzo di exchange privi di KYC o con sede in giurisdizioni FATF grey list; il ricorso a privacy coin come Monero o Zcash; il frazionamento sistematico delle operazioni sotto le soglie di rilevazione; la rapida conversione in stablecoin o in valuta fiat; la movimentazione attraverso marketplace del darknet. La presenza di più di uno di questi indici crea una presunzione di fatto difficilmente superabile.

3.4.3 L'autoriciclaggio

L'autoriciclaggio ex articolo 648-ter.1 del codice penale — introdotto dalla legge 186 del 2014 — si distingue dal riciclaggio ordinario per tre elementi. Primo: il soggetto attivo deve essere lo stesso autore del reato presupposto. Secondo: è richiesta una condotta attiva di 'impiego' — la mera detenzione non è sufficiente. Terzo: è necessario che la condotta 'ostacoli concretamente' l'identificazione della provenienza delittuosa — elemento aggiuntivo rispetto al riciclaggio ordinario.

Nelle cripto-attività, le condotte tipiche di autoriciclaggio includono: la conversione dei proventi in Bitcoin con successivo passaggio attraverso mixer; l'utilizzo di DeFi per generare rendimento sul

capitale illecito; l'acquisto di NFT con proventi di frode. L'ostacolo concreto si dimostra attraverso l'analisi blockchain: il numero di hop tra il wallet originale e quello finale, l'uso di servizi di anonimizzazione intermedi, i passaggi attraverso exchange privi di KYC.

3.5 Questioni processuali ancora aperte

Alcune questioni processuali rilevanti non hanno ancora ricevuto una risposta giurisprudenziale stabile.

La responsabilità per perdita di valore durante il sequestro: i Bitcoin sequestrati e detenuti in forma liquida durante il processo possono subire deprezzamenti significativi (o rivalutazioni). Chi risponde nei confronti dell'imputato assolto? La giurisprudenza civile non ha ancora affrontato specificamente il tema. L'analogia più vicina è Cassazione civile n. 8662/2019 sui titoli azionari sequestrati: il responsabile civile risponde del deprezzamento se imputabile a sua negligenza.

La competenza territoriale per i reati commessi su blockchain rimane incerta. Dove si perfeziona il reato? Dove risiede l'indagato? Dove ha sede il nodo validante? Dove è il server del VASP? La Cassazione penale, Sezione II, con sentenza n. 1200/2019, ha indicato per il riciclaggio il locus commissi delicti nel luogo dove avviene il reimpiego percepito economicamente dall'autore. Ma la questione non è ancora definitivamente risolta.

Il wallet inaccessibile e il diritto al silenzio: l'indagato che afferma di aver perso la seed phrase — o che si rifiuta di rivelarla — non può essere obbligato ad autoincolparsi. Il sequestro rimane 'vuoto'. La soluzione processuale, come già indicato, è la confisca per equivalente. Ma la questione ha implicazioni più ampie sull'effettività della repressione penale in questo settore.

La configurabilità del finanziamento al crimine in capo alla vittima di ransomware che paga: se la vittima paga il riscatto in Bitcoin, commette il reato di finanziamento? La giurisprudenza è ancora divisa. La questione è aperta.

CAPITOLO IV — Profili Civilistici e Patrimoniali

4.1 La natura giuridica delle cripto-attività nel diritto civile italiano

Il diritto civile italiano non ha ancora ricevuto una risposta legislativa chiara sulla natura giuridica delle cripto-attività. La dottrina si divide tra tre teorie principali, ciascuna con implicazioni processuali diverse.

La teoria della cosa mobile, accolta dalla giurisprudenza penale con Cassazione 26807/2021, consente l'applicazione immediata degli strumenti processuali — sequestro, rivendicazione, furto. La critica è che manca la fisicità essenziale del concetto romanistico di 'cosa' e che non vi è 'possesso' nel senso tradizionale dell'articolo 1140 del codice civile. La teoria del bene immateriale, dogmaticamente più coerente con la natura tecnica dell'asset, è prevalente in Germania — dove il BGB è stato interpretato per analogia — e in Francia, che ha riformato il Code civil nel 2022 introducendo una categoria specifica per gli asset digitali. Il limite è che il codice civile italiano non prevede una categoria generale di beni immateriali, e l'opponibilità ai terzi rimane incerta senza una norma espressa. La teoria dello strumento finanziario è applicabile solo ai security token, con piena operatività di TUF e tutele dell'investitore. MiCA ha creato un tertium genus che si colloca tra bene mobile e strumento finanziario, rendendo ancora più complessa la categorizzazione.

> Consiglio operativo: non adottare una tesi in modo dogmatico. Adattare la qualificazione all'obiettivo processuale. In sede penale, la cosa mobile consente il sequestro. In sede civile,

> il bene immateriale supporta il pignoramento e la tutela inibitoria. Ogni sentenza emessa su questo tema costruisce il diritto che ancora manca.

4.2 Smart contract e responsabilità civile

Lo smart contract è un programma informatico che opera su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti — così lo definisce l'articolo 8-ter del D.L. 135/2018 convertito in L. 12/2019. La norma italiana li riconosce ma non li disciplina compiutamente.

Dal punto di vista civilistico, la proposta contrattuale corrisponde al 'deploy' del codice sul blockchain; l'accettazione corrisponde all'interazione con il contratto. La causa deve essere lecita e meritevole di tutela ex articolo 1322 del codice civile — la causa illecita rende nullo lo smart contract come qualsiasi altro contratto. Il codice sorgente è la norma contrattuale, ma l'intenzione delle parti ex articolo 1362 rimane prevalente in caso di contrasto.

Il caso The DAO del 2016 rimane il riferimento giurisprudenziale più citato. Un bug nel codice dello smart contract permise a un soggetto anonimo di sottrarre circa 150 milioni di dollari. La comunità Ethereum decise di effettuare un 'hard fork' — una modifica retroattiva del registro blockchain — per annullare la sottrazione. Dal punto di vista giuridico, questa soluzione tecnica pone domande senza risposta: chi ha il potere di modificare un registro che si proclama immutabile? È ammissibile nel diritto privato italiano una modificazione retroattiva degli effetti contrattuali da parte di un soggetto non identificato?

Sulla responsabilità per malfunzionamento: il bug nel codice genera danno ex articolo 2043 del codice civile a carico dello sviluppatore. Rimane aperta la questione se risponda anche l'auditor che ha certificato il codice, per responsabilità extracontrattuale o contrattuale verso i terzi danneggiati.

4.3 Le cripto-attività nelle successioni mortis causa

Le cripto-attività rientrano nell'asse ereditario del de cuius come beni patrimoniali ex articolo 586 del codice civile. Il valore deve essere dichiarato nella denuncia di successione con applicazione delle aliquote ordinarie dell'imposta di successione, calcolato alla data del decesso ex articolo 474 del codice civile.

La stima effettuata da Coinbase quantifica in circa quattro milioni di Bitcoin — al valore attuale pari a circa 150 miliardi di euro — gli asset digitali permanentemente inaccessibili a causa del decesso dei proprietari senza trasmissione delle chiavi private. Il problema si aggrava ogni anno con la crescita della diffusione.

Per il notaio che redige l'inventario: le competenze tecniche necessarie per identificare e valutare wallet ed exchange non rientrano nella formazione professionale ordinaria. È necessaria una perizia tecnica specialistica. L'inventario ex articolo 769 del codice di procedura civile deve includere la descrizione del tipo di wallet, il nome dell'exchange se custodial, gli indirizzi pubblici noti, il valore alla data del decesso.

La Cassazione civile, con sentenza del 2023, ha stabilito che se l'erede movimenta il wallet del de cuius — anche solo consultandone il saldo — integra accettazione tacita dell'eredità ex articolo 476 del codice civile, con responsabilità illimitata per i debiti ereditari. Questa massima deve essere portata a conoscenza degli eredi prima di qualsiasi interazione con i dispositivi del defunto.

Per i wallet custodial presso exchange: con certificato di morte e atto di notorietà, alcuni exchange rilasciano i fondi agli eredi legittimi. Per i wallet non-custodial in assenza della seed phrase: i Bitcoin sono definitivamente inaccessibili — nessuna azione giudiziaria può recuperarli. La best practice emergente è il 'testamento digitale' o 'testamento tecnologico': un documento che trasmette agli eredi fidati le istruzioni per accedere ai wallet, da custodire in modo sicuro e separato dai device.

4.4 Le cripto-attività nella separazione e nel divorzio

Le cripto-attività sono lo strumento più utilizzato per nascondere il patrimonio in sede di separazione giudiziale. Le caratteristiche che le rendono ideali per questo scopo — pseudonimato, transferibilità globale istantanea, assenza di registrazione in archivi pubblici — sono le stesse che rendono difficile la loro identificazione da parte del coniuge e del giudice.

4.4.1 Regime patrimoniale e divisione

In comunione legale ex articolo 177 del codice civile: le cripto-attività acquistate in costanza di matrimonio sono beni comuni indipendentemente dall'intestazione del wallet. Il diritto alla metà si applica. In separazione dei beni: le cripto rimangono del coniuge acquirente ma possono essere oggetto di assegno divorzile. La valorizzazione è il punto critico: alla data della domanda di separazione? Alla data della sentenza? La prassi più ragionevole è quella di concordare nel verbale di separazione una data di riferimento certa.

4.4.2 Come scoprire le cripto nascoste

I principali strumenti disponibili: ordine di esibizione ex articolo 210 del codice di procedura civile rivolto all'exchange per il rilascio del KYC e dello storico delle transazioni — spesso resistito da exchange esteri; OEI o rogatoria per gli exchange con sede in paesi UE; CTU blockchain con analisi OSINT degli indirizzi noti e cluster analysis per l'identificazione del patrimonio nascosto; la dichiarazione falsa dei redditi — se il coniuge ha omesso le cripto nel modello 730, questa è prova di occultamento (Cassazione civile 2022).

> Dato operativo: il passaggio dall'8% al 18% di italiani con cripto-attività registrato tra il 2022 e il 2023 (dati CONSOB 2024) significa che in circa una separazione su cinque trattata oggi ci sono cripto-attività da qualche parte. La verifica sistematica dei movimenti bancari del triennio precedente per identificare acquisti su exchange è diventata prassi necessaria nelle CTU finanziarie.

4.4.3 Misure cautelari e processuali

Il sequestro conservativo ex articolo 671 del codice di procedura civile sul wallet presso l'exchange è possibile in presenza di fumus boni iuris e periculum. L'ordine di blocco anticipatorio ex articolo 700 del codice di procedura civile è lo strumento d'urgenza quando il coniuge stia per trasferire i fondi ante-separazione. L'azione revocatoria ex articolo 2901 del codice civile è applicabile se le cripto sono già state trasferite a terzi per frodare le ragioni del coniuge. Il trasferimento forzoso: il giudice può ordinare il trasferimento della metà dei Bitcoin al coniuge avente diritto ex articolo 709-ter del codice di procedura civile, con astreinte ex articolo 614-bis per l'inadempimento.

4.5 Tutela del creditore, pignoramento e fallimento

Per il pignoramento di cripto-attività ex articolo 543 del codice di procedura civile: l'exchange è il terzo pignorato con obbligo di dichiarazione ex articolo 547, da notificarsi con ordinaria modalità. Per l'exchange estero che non risponde: OEI per i paesi UE, rogatoria internazionale per gli altri. Per il wallet non-custodial: il pignoramento presso terzi non è applicabile — occorre il pignoramento diretto del device fisico in sede esecutiva ex articolo 513, con nomina di un ausiliario tecnico.

Nel fallimento e nella crisi d'impresa ex D.Lgs. 14/2019: il curatore ha l'obbligo di cercare attivamente le cripto-attività del fallito, inviando richieste a tutti gli exchange italiani e OEI per quelli europei. I trasferimenti ante-fallimento sono revocabili nelle condizioni ordinarie. Se dolosi — e la blockchain fornisce la prova del trasferimento con data e ora certa — configurano bancarotta fraudolenta per occultamento di attivi ex articolo 216 della legge fallimentare.

CAPITOLO V — Il Sistema di Prevenzione AML

5.1 L'architettura normativa: dalla piramide FATF all'Italia

Il sistema di prevenzione antiriciclaggio applicabile alle cripto-attività si struttura su quattro livelli normativi sovrapposti.

Al vertice: il GAFI (Gruppo di Azione Finanziaria Internazionale) con le sue 40 Raccomandazioni. La Raccomandazione 15, aggiornata nel 2019, è la svolta: i Virtual Asset Service Provider — VASP — devono applicare le stesse misure antiriciclaggio delle banche tradizionali. La Raccomandazione 16 — Travel Rule — impone la trasmissione dei dati dell'ordinante e del beneficiario per ogni trasferimento di asset virtuali.

Secondo livello: il diritto dell'Unione Europea. Il Regolamento MiCA (2023/1114), il Regolamento Transfer of Funds (2023/1113 — Travel Rule), e l'AML Package 2024 che include il Regolamento AML, la Sesta Direttiva AML e l'istituzione dell'Autorità Europea AML (AMLA) con sede a Francoforte, operativa dal 2025 con potere di vigilanza diretta sui VASP.

Terzo livello: la normativa italiana. Il D.Lgs. 231/2007, modificato dal D.Lgs. 125/2019 di recepimento della V Direttiva AML, individua i soggetti obbligati in ambito cripto: exchange, custodial wallet provider, broker e dealer, marketplace NFT di volume rilevante, professionisti che accettano pagamenti in cripto oltre soglia. Il D.Lgs. 129/2024 ha attuato MiCA designando CONSOB e Banca d'Italia come autorità competenti. I provvedimenti OAM e le circolari UIF completano il quadro.

5.2 Gli obblighi dei VASP: KYC, adeguata verifica, SOS

5.2.1 Adeguata verifica ordinaria (CDD)

L'adeguata verifica ordinaria richiede: identificazione del cliente con documento di identità e verifica del volto (selfie); verifica della titolarità effettiva (chi controlla davvero il wallet); comprensione dello scopo e della natura del rapporto; monitoraggio continuo delle transazioni con generazione di alert automatici su pattern anomali; aggiornamento periodico del profilo cliente ogni 1-3 anni.

5.2.2 Adeguata verifica rafforzata (EDD)

L'adeguata verifica rafforzata è obbligatoria per: persone politicamente esposte (PEP) e loro familiari e stretti associati; clienti provenienti da paesi nella grey list o black list FATF (es. Yemen, Iran, Corea del Nord); transazioni superiori a 10.000 euro o pattern ad alto rischio. Richiede approvazione del senior management per instaurare o continuare il rapporto e verifica documentale dell'origine dei fondi.

5.2.3 Rilevanza processuale del KYC

Per il magistrato, il KYC è la prova regina: collega un indirizzo blockchain — che di per sé è solo una stringa alfanumerica — a una persona fisica con nome, cognome, documento di identità, numero di telefono e indirizzo fisico. Il decreto di esibizione ex articolo 256 del codice di procedura penale rivolto all'exchange produce il fascicolo cliente completo. Se il KYC è falso: ulteriore reato ex articolo 495 del codice penale per falsa dichiarazione a pubblico ufficiale. Se il VASP non ha effettuato il KYC: responsabilità penale del compliance officer ex articolo 55 del D.Lgs. 231/2007. Il KYC incompleto o superficiale è di per sé indizio di dolo nell'exchange compiacente.

5.3 La Travel Rule: svolta rivoluzionaria per le indagini

Il Regolamento UE 2023/1113 (Transfer of Funds Regulation), in vigore dal 30 dicembre 2024, introduce la Travel Rule per i trasferimenti di cripto-attività senza soglia minima. Per ogni

trasferimento tra VASP, il VASP del mittente deve trasmettere al VASP del beneficiario: nome e cognome dell'ordinante; indirizzo del wallet o numero di conto; più almeno un dato aggiuntivo tra indirizzo fisico, data di nascita e numero di documento di identità. Il VASP destinatario deve verificare i dati ricevuti e bloccare il trasferimento se i dati mancano o se il wallet figura in una lista di sanzioni (OFAC, EU, ONU).

> *«A decorrere dal 30 dicembre 2024, i prestatori di servizi per le cripto-attività devono garantire che i trasferimenti di cripto-attività siano accompagnati dalle informazioni sull'ordinante e sul beneficiario e che tali informazioni restino a disposizione per le autorità competenti ai fini della prevenzione, dell'individuazione e dell'investigazione del riciclaggio di denaro e del finanziamento del terrorismo.» — Reg. UE 2023/1113, considerando (1)*

Prima della Travel Rule: per identificare il mittente di un trasferimento crypto, l'investigatore doveva fare una richiesta separata all'exchange del mittente — spesso estero — con tempi lunghi e esiti incerti. Dopo la Travel Rule: i dati del mittente sono già nel fascicolo dell'exchange destinatario dal momento del trasferimento. Una SOS generata per violazione della Travel Rule — dati mancanti, wallet sanzionato — costituisce già di per sé un indizio di tentativo di elusione degli obblighi AML, rilevante ex articolo 648-bis del codice penale.

Il punto critico è rappresentato dai wallet non custodial — MetaMask, hardware wallet, wallet DeFi. Per questi wallet non vi è un VASP controparte. Il Regolamento impone la verifica mediante proof of ownership — una firma crittografica che dimostra il controllo del wallet senza rivelarne la chiave privata. Il dibattito tra operatori e regolatori sull'applicazione pratica di questo obbligo è ancora aperto.

5.4 Gli indicatori di anomalia UIF 2022

La UIF — Unità di Informazione Finanziaria per l'Italia — ha emanato il 12 maggio 2022 un provvedimento recante 34 indicatori di anomalia specifici per le cripto-attività. I dieci più rilevanti per l'attività giudiziaria sono i seguenti.

IND.1 — Frazionamento: operazioni ripetute appena sotto le soglie di rilevazione — strutturazione classica. IND.2 — Exchange no-KYC: utilizzo di piattaforme prive di adeguata verifica o con sede in giurisdizioni FATF grey list. IND.3 — Conversione immediata: cripto ricevute convertite in stablecoin o in euro nel giro di poche ore senza apparente scopo. IND.4 — Uso di mixer: transazione che passa per Tornado Cash, Chipmixer o servizi analoghi: intento di rompere il collegamento blockchain. IND.5 — Privacy coin: uso di Monero (XMR), Zcash (ZEC) o Dash con funzioni di privacy attivate. IND.6 — Darknet origin: wallet con transazioni provenienti da indirizzi associati a marketplace del darknet. IND.7 — Wallet sanzionati: transazione con wallet in lista OFAC, EU Sanctions o ONU. IND.8 — Profilo incongruente: volumi transazionali incompatibili con reddito o patrimonio dichiarato in fase KYC. IND.9 — Operatività ATM crypto: uso frequente di ATM Bitcoin per conversioni cash-to-crypto o viceversa. IND.10 — Smart contract anomali: interazione con smart contract che implementano funzioni di hacking, phishing o drenaggio forzato di fondi.

> Come leggere la SOS nel fascicolo: verificare il codice dell'indicatore di anomalia (indica cosa ha attivato la segnalazione), la data (quando è stata rilevata l'anomalia), il soggetto segnalante (quale VASP ha segnalato), gli allegati KYC. La SOS non è prova del reato ma è il punto di partenza investigativo. Quando più SOS di diversi VASP vengono correlate sullo stesso soggetto o cluster di indirizzi, il quadro probatorio diventa molto solido.

5.5 Il Registro OAM e le responsabilità dei VASP non registrati

Dal 2022, tutti i prestatori di servizi relativi all'utilizzo di valuta virtuale operanti in Italia devono essere iscritti al Registro OAM (Organismo Agenti e Mediatori) entro 60 giorni dall'avvio dell'attività. Dal 2025, è richiesta la licenza CASP ex MiCA per i servizi transfrontalieri UE. Il Registro è pubblico e consultabile gratuitamente su oam.it.

Le conseguenze per il VASP non registrato sono articolate su tre livelli. Livello amministrativo: sanzione ex articolo 17-bis D.Lgs. 231/2007 da 5.000 a 700.000 euro. Livello penale: abusivismo finanziario ex articolo 166 TUF con reclusione da uno a otto anni, se offre servizi di investimento; responsabilità degli amministratori per omessa vigilanza. Livello penale aggravato: concorso in riciclaggio se il VASP abusivo è consapevole dell'origine illecita dei fondi trattati.

Gli strumenti investigativi per il PM: verifica immediata su oam.it; lista nera CONSOB dei siti non autorizzati, aggiornata settimanalmente; registro EBA dei CASP autorizzati in tutta l'UE; collaborazione con Guardia di Finanza (GICO) e Polizia Postale per OSINT sul VASP; undercover purchase — acquisto da agente UC per documentare l'assenza di KYC; sequestro d'urgenza dell'infrastruttura informatica ex articolo 321 del codice di procedura penale.

CAPITOLO VI — La Posizione delle Autorità Italiane

6.1 CONSOB: i moniti ufficiali

La CONSOB ha assunto nel corso del 2024-2025 posizioni ufficiali di crescente severità nei confronti delle cripto-attività, che meritano di essere conosciute dal magistrato per la loro rilevanza nella valutazione del danno ai risparmiatori e nella interpretazione delle condotte di offerta al pubblico.

Il 22 novembre 2024, il Commissario CONSOB Federico Cornelli, intervenendo al convegno 'Le scelte degli investitori italiani tra consulenza e sostenibilità', ha pronunciato la dichiarazione ufficiale più diretta mai rilasciata da un'autorità di vigilanza italiana su questo asset class.

> *«I bitcoin e le altre criptovalute sono strumenti altamente speculativi. Sotto non c'è nulla. Non c'è un debitore. Se mai un giorno dovesse scoppiare la bolla, nessuno venga a chiedere risarcimenti alle Autorità o ai governi.» — Commissario CONSOB Federico Cornelli, 22 novembre 2024*

Il medesimo intervento ha evidenziato dati di grande rilievo per la valutazione della condizione di vulnerabilità delle vittime di frodi in cripto: tra il 2022 e il 2023 la percentuale di italiani con cripto-attività in portafoglio è più che raddoppiata, passando dall'8% al 18%. La fonte informativa prevalente sono i social network (36% degli intervistati), con una sovraesposizione dei soggetti più vulnerabili: giovani, donne, persone con minore alfabetizzazione finanziaria.

Il 6 marzo 2025, Banca d'Italia e CONSOB hanno emesso una comunicazione congiunta rivolta alle società di revisione e ai revisori legali, che richiede particolare attenzione nell'accettazione e nello svolgimento di incarichi relativi a società con esposizioni rilevanti in cripto-attività. Il documento richiama il warning ESMA del 13 dicembre 2024 che definisce le cripto-attività 'altamente speculative e volatili' e impone la verifica rafforzata dell'integrità del cliente e del modello di business.

Nel luglio 2025, il presidente CONSOB Paolo Savona, audito dalla Commissione parlamentare di inchiesta sul sistema bancario, ha dichiarato: 'Gli italiani hanno da parte oltre seimila miliardi di euro. Su questo risparmio incombe la minaccia cripto.' Il presidente ha proposto la creazione di un euro digitale non remunerato e di un safe asset BCE come risposta competitiva al fenomeno.

6.2 Banca d'Italia: la posizione ufficiale

Banca d'Italia ha espresso sin dal 2015 — con comunicazioni aggiornate nel 2022 — una posizione netta: le valute virtuali non sono moneta legale, non sono emesse né garantite da autorità pubblica, non esiste un quadro normativo di tutela degli utenti paragonabile a quello previsto per i depositi bancari o gli strumenti finanziari.

Con l'attuazione di MiCA tramite D.Lgs. 129/2024, Banca d'Italia ha assunto il ruolo di autorità competente per i requisiti prudenziali e l'antiriciclaggio dei CASP, mentre CONSOB vigila sulla trasparenza e la condotta. I poteri di vigilanza includono: autorizzazione e revoca dell'autorizzazione ai CASP; ispezioni e sanzioni; ordini di cessazione dell'attività per i VASP non conformi.

CAPITOLO VII — Il Quadro Normativo di Riferimento

7.1 Normativa dell'Unione Europea

Il corpus normativo europeo applicabile alle cripto-attività si è consolidato nel 2023-2024 con l'adozione di un sistema organico che non ha precedenti a livello globale.

- Reg. (UE) 2023/1114 — MiCA (Markets in Crypto-Assets): primo quadro normativo organico per i mercati delle cripto-attività. In vigore dal giugno 2024 per ART e EMT, dal dicembre 2024 per tutti i CASP.
- Reg. (UE) 2023/1113 — TFR (Transfer of Funds Regulation): Travel Rule estesa alle cripto-attività senza soglia minima, in vigore dal 30 dicembre 2024.
- AML Package 2024: Regolamento AML (applicazione diretta), VI Direttiva AML, istituzione AMLA con sede a Francoforte, operativa 2025.
- Dir. (UE) 2018/843 — V Direttiva AML: prima inclusione dei VASP tra i soggetti obbligati agli obblighi antiriciclaggio.
- CGUE C-264/14 (Hedqvist, 2015): Bitcoin equiparato a valuta ai fini IVA — operazioni di cambio esenti.

7.2 Normativa italiana

- D.Lgs. 231/2007, come modificato dal D.Lgs. 125/2019: obblighi AML per i VASP, definizione di valuta virtuale, registro OAM.
- D.Lgs. 129/2024: attuazione MiCA in Italia. Designazione CONSOB (trasparenza e condotta) e Banca d'Italia (requisiti prudenziali e AML) come autorità competenti.
- L. 197/2022 (Legge di Bilancio 2023): tassazione delle plusvalenze su cripto-attività al 26% per eccedenze superiori a 2.000 euro annui.
- Circolari UIF 2022: 34 indicatori di anomalia specifici per le cripto-attività (Provvedimento del 12 maggio 2022).
- Provvedimenti OAM: registro pubblico dei VASP operanti in Italia, consultabile su oam.it.
- D.Lgs. 108/2017: recepimento della Direttiva OEI — strumento per la cooperazione internazionale con i paesi UE.

7.3 Giurisprudenza essenziale

Le sentenze di riferimento che il magistrato deve conoscere, in ordine di rilevanza sistematica.

- Cass. pen. Sez. II, 25 giugno 2021, n. 26807: Bitcoin qualificabile come cosa mobile ex art. 624 c.p. — suscettibile di sequestro preventivo ex art. 321 c.p.p. Leading case assoluto.
- Cass. pen. Sez. II, 14 giugno 2021, n. 23017: il dolo eventuale è sufficiente per il riciclaggio — chi usa un mixer sa probabilmente di anonimizzare fondi illeciti.

- Cass. pen. Sez. II, n. 34895/2022: lo swap tra cripto diverse integra la condotta di sostituzione ex art. 648-bis c.p.
- Cass. pen. Sez. II, n. 1200/2019: per il riciclaggio, il locus commissi delicti è dove avviene il reimpiego percepito economicamente dall'autore.
- CGUE C-264/14, Hedqvist, 22 ottobre 2015: Bitcoin equiparato a valuta ai fini IVA — operazioni di cambio esenti.
- Cass. civ., 2023: la movimentazione del wallet del de cuius da parte dell'erede integra accettazione tacita ex art. 476 c.c.
- Cass. civ. Sez. I, 2022: sulla natura giuridica delle cripto-attività nell'ordinamento civile italiano.
- Trib. Verona, 2019: sulla validità del pagamento in Bitcoin tra parti contraenti.
- Trib. Brescia, 2023: il gestore di un DEX italiano può essere ritenuto responsabile se non ha adottato misure KYC adeguate.

CAPITOLO VIII — Casi Pratici per la Discussione

Nella parte finale del corso sono stati presentati quattro casi pratici destinati alla discussione con la platea. Si tratta di situazioni già affrontate dalla magistratura italiana o che presentano elementi di elevata probabilità di ricorrenza nei fascicoli futuri.

Caso A — Sequestro urgente di Bitcoin su exchange estero

Un indagato per traffico di stupefacenti detiene 12 BTC su un exchange con sede a Malta (soggetto a MiCA). Il PM apprende dell'esistenza del wallet da una SOS correlata con l'attività investigativa in corso. Come si procede al sequestro preventivo?

Soluzione operativa: verifica immediata dell'iscrizione dell'exchange nel registro EBA dei CASP autorizzati (se iscritto, è soggetto agli obblighi MiCA e risponde agli ordini delle autorità). Emissione del decreto di sequestro ex articolo 321 c.p.p. con richiesta di blocco immediato dell'account. Contemporaneamente, OEI ex D.Lgs. 108/2017 verso Malta per il formale congelamento. Nel frattempo, attivazione del canale informale UIF-Egmont per ottenere intelligence immediata (24-72 ore) senza attendere i tempi formali dell'OEI. Norme applicabili: art. 321 c.p.p., OEI, MiCA CASP.

Caso B — La prova digitale in udienza: il printscreen di Etherscan

Il PM produce in udienza un printscreen di Etherscan — il blockchain explorer per la rete Ethereum — che mostra le transazioni dell'imputato. La difesa eccepisce la mancata verifica dell'integrità del documento informatico e la non autenticità della copia. Come si pronuncia il GUP?

Analisi: il printscreen è un documento informatico ex articolo 234 del codice di procedura penale. La questione è l'integrità: un printscreen può essere manipolato. La soluzione corretta è l'acquisizione forense della pagina web con calcolo dell'hash del file al momento dell'acquisizione, in conformità alla norma ISO/IEC 27037:2012 sull'acquisizione della prova digitale. In mancanza di questa certificazione, il printscreen è prova documentale di valore indiziario. La correttezza dell'informazione può essere verificata indipendentemente da chiunque tramite lo stesso blockchain explorer. Norme applicabili: art. 234 c.p.p., art. 254-bis c.p.p., ISO/IEC 27037.

Caso C — Autoriciclaggio DeFi e revocatoria

Un truffatore converte i proventi di una truffa online (500.000 euro) in ETH su Uniswap, poi in USDT tramite uno swap cross-chain, e infine preleva su un conto bancario intestato alla moglie. La moglie sostiene di non sapere dell'origine illecita. Individuare le fattispecie penali e civili applicabili.

Analisi penale: l'autore risponde di autoriciclaggio ex articolo 648-ter.1 c.p. (stesso soggetto del predicate offense; condotta attiva di impiego; ostacolo concreto dimostrabile dall'analisi blockchain dei hop ETH→USDT→conto). Il P.M. deve verificare se la moglie ha avuto consapevolezza: in caso affermativo, concorso nel 648-ter.1 o ricettazione. Analisi civile: azione revocatoria ex articolo 2901 c.c. sul trasferimento al conto della moglie (atto a titolo gratuito; pregiudizio del creditore — in questo caso lo Stato per la confisca; consapevolezza del debitore dell'effetto pregiudizievole). La blockchain fornisce la catena completa: dal wallet del truffatore alla stablecoin, all'exchange, al bonifico bancario. Norme applicabili: art. 648-ter.1 c.p., art. 2901 c.c., D.Lgs. 231/2007.

Caso D — Successione con Bitcoin e seed non trovata

Il de cuius muore lasciando 5 BTC (valore corrente circa 400.000 euro) di cui solo lui conosceva il seed. Gli eredi non trovano né il device né la seed phrase. Come si gestisce la successione?

Analisi: i 5 BTC rientrano nell'asse ereditario e devono essere dichiarati nella denuncia di successione al valore alla data del decesso. Prima di dichiarare la perdita, seguire questo percorso: ricerca della seed phrase in forma cartacea (taccuino, cassaforte, documento nascosto); ricerca del device fisico (hardware wallet, smartphone); verifica di tutti gli exchange custodial con certificato di morte e atto di notorietà; ricerca di eventuali wallet manager digitali (LastPass, 1Password) o cloud backup. Se il wallet è custodial presso exchange: con le credenziali del de cuius o procedura di recupero account. Se non custodial e seed non trovata: i Bitcoin sono inaccessibili. L'asse si riduce a zero per questa componente. Il notaio deve documentare il tentativo di recupero nel verbale di inventario. Norme applicabili: art. 587 c.c., CTU blockchain, denuncia di successione ex D.Lgs. 346/1990.

CAPITOLO IX — Conclusioni e Prospettive

9.1 Il paradosso di Bitcoin e le implicazioni per il magistrato

Bitcoin e le cripto-attività incarnano un paradosso che il magistrato deve tenere sempre presente: sono nate come strumento di libertà — per sottrarre il denaro al controllo dei governi e delle banche — e sono diventate simultaneamente strumento di investimento speculativo, riserva di valore alternativa, e strumento di crimine. Queste tre anime coesistono nello stesso asset. Il fascicolo che arriva sulla scrivania può contenere qualunque delle tre.

Il paradosso investigativo è ancora più acuto: i criminali hanno adottato Bitcoin convinti di stare usando uno strumento anonimo. In realtà, la blockchain è il registro più trasparente e permanente che esista. Ogni transazione è pubblica, immutabile, verificabile da chiunque, per sempre. Pseudonimato non è anonimato. Bitcoin non associa le transazioni a un nome — questo è il pseudonimato — ma le associa a un indirizzo. E quell'indirizzo, appena viene collegato a una persona fisica — tramite il KYC di un exchange, tramite un IP di connessione, tramite un hardware wallet trovato in perquisizione — diventa una prova schiacciante.

La blockchain è il testimone più affidabile che esiste: non mente, non dimentica, non può essere corrotto e non si contraddice. Il compito del magistrato non è sulla blockchain — è nel collegare ciò che la blockchain mostra a una persona fisica. È lì che si vince o si perde il procedimento.

9.2 Le questioni aperte che attendono risposta giurisprudenziale

Il corso ha evidenziato numerose questioni che la giurisprudenza non ha ancora definitivamente risolto e su cui ogni sentenza contribuisce a costruire il diritto.

In ambito penale: la competenza territoriale per i reati commessi su blockchain; la responsabilità per perdita di valore durante il sequestro; la configurabilità del finanziamento al crimine in capo alla vittima che paga il riscatto ransomware; i criteri di nomina del custode giudiziario di cripto-attività; l'obbligo di autoincolpazione per la rivelazione della seed phrase.

In ambito civile: la qualificazione dei token di governance come strumenti partecipativi; i criteri di responsabilità del liquidity provider DeFi; la tutela del consumatore in caso di perdita da hack di smart contract; i criteri di valorizzazione delle cripto in sede successoria e divorzile.

In ambito AML: l'efficacia pratica della Travel Rule per i wallet non custodial; la qualificazione del semplice uso di mixer come indizio di dolo; il perimetro di responsabilità dell'exchange che non blocca una transazione anomala.

9.3 Il ruolo della magistratura nella costruzione del diritto

Il diritto delle cripto-attività è un diritto in costruzione. La velocità dell'evoluzione tecnologica supera di gran lunga quella del legislatore, a livello sia nazionale sia europeo. In questo contesto, la giurisprudenza svolge un ruolo creativo che va ben oltre la mera applicazione della norma.

Ogni sentenza che qualifica la natura di un NFT, che applica la confisca per equivalente a un wallet inaccessibile, che ammette la prova blockchain in sede civile, che definisce i criteri del dolo eventuale per il riciclaggio cripto, è un mattone di un edificio che ancora non esiste. Non è un'iperbole: è la realtà della fase storica in cui ci troviamo.

La Scuola Superiore della Magistratura ha ritenuto urgente e necessaria questa formazione. I dati confermano la scelta: il numero di procedimenti che coinvolgono cripto-attività è in crescita esponenziale, gli strumenti normativi si moltiplicano, e la competenza tecnica del magistrato è l'unico presidio contro l'errore processuale in un settore dove l'errore tecnico può essere irreversibile.

> *«Il giurista del XXI secolo non può ignorare la tecnologia. La blockchain è già nei fascicoli processuali.» — Luigi Patruno, SSM Lecce, 15 aprile 2026*

APPENDICE — Riferimenti Normativi e Giurisprudenziali Completi

A. Normativa dell'Unione Europea

- Reg. (UE) 2023/1114 — Regolamento MiCA
- Reg. (UE) 2023/1113 — Regolamento Transfer of Funds (Travel Rule)
- Dir. (UE) 2018/843 — V Direttiva AML
- Reg. (UE) 2024/1624 — Regolamento AML (AML Package)
- Dir. (UE) 2024/1640 — VI Direttiva AML
- Reg. (UE) 2024/1620 — Istituzione AMLA

B. Normativa italiana

- D.Lgs. 21 novembre 2007, n. 231 — Antiriciclaggio
- D.Lgs. 4 ottobre 2019, n. 125 — Recepimento V Direttiva AML
- D.Lgs. 5 settembre 2024, n. 129 — Attuazione MiCA in Italia
- L. 29 dicembre 2022, n. 197 (Legge di Bilancio 2023) — Tassazione cripto
- D.Lgs. 5 giugno 2017, n. 108 — Ordine Europeo di Indagine
- D.L. 14 dicembre 2018, n. 135, conv. L. 11 febbraio 2019, n. 12 — Smart contract
- UIF, Provvedimento 12 maggio 2022 — 34 Indicatori di anomalia cripto
- Circolare AdE 30/E del 2023 — Trattamento fiscale cripto-attività

C. Giurisprudenza

- Cass. pen. Sez. II, 25 giugno 2021, n. 26807 — Bitcoin come cosa mobile
- Cass. pen. Sez. II, 14 giugno 2021, n. 23017 — Dolo eventuale nel riciclaggio
- Cass. pen. Sez. II, n. 34895/2022 — Swap crypto come sostituzione ex 648-bis
- Cass. pen. Sez. II, n. 1200/2019 — Locus commissi delicti per riciclaggio
- CGUE C-264/14, Hedqvist, 22 ottobre 2015 — Bitcoin ed esenzione IVA
- Cass. civ., 2023 — Accettazione tacita eredità e movimentazione wallet
- Cass. civ. Sez. I, 2022 — Natura giuridica cripto-attività
- Trib. Verona, 2019 — Validità pagamento in Bitcoin
- Trib. Brescia, 2023 — Responsabilità gestore DEX
- Trib. Milano, ord. 2022 — Nomina custode giudiziario e conversione immediata in EUR

D. Dottrina e Prassi

- GAFI, Guidance for a Risk-Based Approach to Virtual Assets and VASPs, 2021
- Europol, Internet Organised Crime Threat Assessment (IOCTA), 2023
- ESMA, Warning on crypto-assets, 13 dicembre 2024
- Banca d'Italia/CONSOB, Comunicazione congiunta, 6 marzo 2025
- CONSOB, Commissario Cornelli, Comunicato stampa 22 novembre 2024
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 31 ottobre 2008
- Eric Hughes, A Cypherpunk's Manifesto, 9 marzo 1993

Fine della Relazione Formativa

Corso D26205 — SSM Formazione Decentrata Corte d'Appello di Lecce — 15 aprile 2026

Dr. Luigi Patruno | Dr. Silverio Greco | Magistrato Formatore Dott. Antonio Ivan Natali