

CRYPTO-FORENSICS E DIFESA PENALE

*Come Tracciare, Bloccare e Recuperare Asset Digitali
Sottratti*

Manuale Pratico per Vittime, Professionisti e Investigatori

Avv. Alessandro Santoro

Penalista Specializzato in Diritto delle Criptovalute

Studio Legale Santoro — Bologna, Piazza Galileo n. 5

www.avvocatosantorobologna.com

Note dell'Editore e Avvertenze Legali

Le informazioni contenute in questo manuale hanno carattere esclusivamente informativo e divulgativo. Non costituiscono in alcun modo consulenza legale personalizzata. Ogni caso di truffa su criptovalute presenta caratteristiche uniche che richiedono una valutazione individuale da parte di un professionista qualificato.

L'autore declina ogni responsabilità per l'utilizzo delle informazioni contenute in questo volume. Per assistenza legale specifica, si consiglia di contattare direttamente lo Studio Legale Santoro.

I casi studio presentati in questo volume sono tratti da vicende di pubblico dominio, da sentenze pubblicate e da episodi riportati dalla stampa specializzata. Non si tratta di casi seguiti personalmente dall'autore: vengono analizzati a scopo puramente didattico e illustrativo. Qualsiasi riferimento a persone fisiche reali è puramente casuale.

Prima edizione — 2026

Copyright © 2026 Avv. Alessandro Santoro — Tutti i diritti riservati

*A tutte le vittime che hanno creduto in un sogno
e si sono ritrovate a combattere una battaglia che non avevano
scelto.*

Questo libro nasce per voi.

Prefazione

Ho scritto questo libro perché ogni settimana, nella mia sede di Bologna, incontro persone distrutte. Non da malattie o lutti, ma da una truffa digitale. Medici, insegnanti, pensionati, imprenditori: persone intelligenti, colte, che hanno creduto in una promessa di futuro migliore e si sono ritrovate con i conti bancari svuotati, i risparmi di una vita scomparsi in una serie di transazioni su una blockchain che non sapevano nemmeno come leggere.

La prima cosa che mi dicono, quasi sempre, è: “Avvocato, so già che non c’è niente da fare. I Bitcoin non si recuperano.” Quella frase mi ha sempre fatto male. Non perché sia falsa in assoluto, ma perché nasce da una rassegnazione costruita ad arte dai criminali stessi, che hanno tutto l’interesse a far credere alle vittime che resistere sia inutile.

La verità è diversa e più complessa. La blockchain non è un paradiso dell’impunità: è il registro più trasparente mai creato dall’uomo. Ogni transazione è scritta per sempre, immutabile, pubblica. Il problema non è la tracciabilità: il problema è la competenza necessaria per leggere quelle tracce e trasformarle in azione legale concreta.

Questo manuale nasce dall’incrocio di due mondi che raramente si parlano: la tecnologia blockchain e il diritto penale italiano. Non è un libro per esperti di informatica, né un trattato giuridico per addetti ai lavori. È una guida per chiunque abbia subito una truffa crypto, per chi voglia difendersi, e per i professionisti legali che intendono specializzarsi in questo settore in rapida evoluzione.

Ho strutturato il volume in cinque parti, dalla comprensione del crimine alla strategia di recupero, con casi di studio tratti da vicende reali di pubblico dominio, strumenti pratici e checklist operative. Ogni capitolo può essere letto autonomamente, ma il filo conduttore è sempre lo stesso: conoscere è il primo passo per combattere.

Avv. Alessandro Santoro — Bologna, 2026

Indice

Prefazione

Introduzione — Il Far West Digitale

PARTE PRIMA — ANATOMIA DEL CRIMINE

Capitolo 1 — L'ingegneria sociale dietro le truffe crypto

Capitolo 2 — Le nuove frontiere della frode: AI, Deepfake e NFT

Capitolo 3 — Il profilo psicologico della vittima

PARTE SECONDA — LA SCIENZA DELLA BLOCKCHAIN

Capitolo 4 — Fondamenti di Chain Analysis Forense

Capitolo 5 — Gli strumenti del tracciamento professionale

Capitolo 6 — DeFi, Mixer e Privacy Coins

PARTE TERZA — LA STRATEGIA LEGALE

Capitolo 7 — La querela tecnico-giuridica: come costruirla per vincere

Capitolo 8 — Il quadro normativo: MiCA, D.Lgs. 231, TUF

Capitolo 9 — Giurisprudenza rilevante

Capitolo 10 — Misure cautelari e sequestri d'urgenza

PARTE QUARTA — IL CONFRONTO INTERNAZIONALE

Capitolo 11 — Gli Exchange e i protocolli di blocco

Capitolo 12 — OIE, Rogatorie e cooperazione internazionale

Capitolo 13 — Le giurisdizioni friendly e quelle ostili

PARTE QUINTA — CASI REALI E LEZIONI APPRESE

Capitolo 14 — Casi di studio tratti dalla cronaca

Capitolo 15 — Gli errori più comuni delle vittime

Conclusioni — Il futuro della giustizia digitale

APPENDICI

Appendice A — Checklist d'emergenza

Appendice B — Glossario tecnico

Appendice C — Normativa di riferimento

Appendice D — Risorse utili e contatti

Introduzione

Il Far West Digitale e la Necessità di una Nuova Difesa

Il mondo delle criptovalute è spesso descritto come una terra senza legge. Per anni, il mito dell'anonimato della Blockchain ha rassicurato i criminali e scoraggiato le vittime. "I Bitcoin non si possono tracciare": questa è la frase che sento ripetere ogni giorno dai clienti che arrivano nel mio studio, spesso dopo aver già tentato invano una denuncia generica.

Questo manuale nasce per smentire questi miti e per fornire una mappa in un territorio che molti considerano inesplorato. La Blockchain non è un buco nero: è il registro più trasparente e immutabile mai creato dall'uomo. Il paradosso del criminale informatico è che, mentre crede di agire nell'ombra, sta scrivendo la propria confessione su un muro digitale che non potrà mai essere cancellato.

Il problema del recupero non è la tracciabilità in sé, ma la capacità tecnica di interpretare i dati grezzi e la competenza legale per trasformare quelle stringhe alfanumeriche in prove forensi accettabili da una Procura della Repubblica.

In queste pagine esploreremo come la Crypto-Forensics incontra la Difesa Penale, offrendo una guida strategica per chi ha subito il furto dei propri risparmi digitali. Non troverete promesse miracolose: troverete metodo, strumenti e la verità su ciò che è realisticamente possibile ottenere attraverso il sistema giudiziario.

PARTE PRIMA

ANATOMIA DEL CRIMINE

Comprendere il nemico è il primo passo per combatterlo

Capitolo 1

Anatomia della Truffa: L'Ingegneria Sociale dietro il Crimine Informatico

Le truffe legate al trading di criptovalute non sono semplici errori tecnici: sono architetture criminali studiate con precisione chirurgica per colpire i due punti deboli di ogni essere umano, ovvero la speranza e la fiducia. Non stiamo parlando di hacker isolati, ma di vere e proprie organizzazioni transnazionali con dipartimenti marketing, call center e analisti finanziari dedicati alla frode.

1.1 Il Pig Butchering: L'Inganno della Lunga Durata

Il termine, di origine asiatica, descrive il processo di ingrasso del maiale prima della macellazione. Il truffatore non chiede denaro subito. Costruisce una relazione che può durare mesi: si presenta come un professionista di successo, mostra screenshot di guadagni straordinari, instaura un rapporto di fiducia profondo. Solo quando la vittima è emotivamente dipendente viene spinta a investire su una piattaforma interamente controllata dai criminali.

Il primo prelievo viene spesso autorizzato per dare l'illusione assoluta di sicurezza. Questo è il momento più pericoloso: la vittima è convinta che il sistema funzioni e investe capitali ancora più ingenti, spesso derivanti da prestiti bancari, vendita di immobili o liquidazione di fondi pensione.

1.2 I Fake Broker e le Piattaforme Specchio

Molti clienti hanno interagito, senza saperlo, con un videogioco finanziario. Le piattaforme fraudolente utilizzano software manipolati in cui i grafici mostrano profitti costanti e crescenti. La vittima vede il proprio saldo aumentare quotidianamente, ma quei numeri sono solo pixel privi di qualsiasi controvalore reale. I fondi vengono trasferiti ai wallet dei truffatori nel momento stesso del primo deposito.

1.3 La Trappola della Tassa di Sblocco

Quando la vittima tenta di prelevare, la piattaforma congela i fondi. Un sedicente ufficio di compliance comunica che, per motivi di Antiriciclaggio o per ottemperare a normative fiscali governative, è necessario versare anticipatamente una tassa pari al 20-26% del capitale da prelevare.

NOTA LEGALE FONDAMENTALE: Nessun Exchange legittimo o autorità fiscale richiede un pagamento preventivo esterno per permettere un prelievo. Le imposte si pagano in sede di dichiarazione dei redditi, mai come condizione per accedere ai propri fondi. Qualsiasi richiesta di questo tipo è una truffa.

1.4 Il Romance Scam Evoluto

Il truffatore costruisce una relazione sentimentale autentica protratta per mesi, creando un legame emotivo profondo con la vittima. Solo successivamente introduce il tema degli investimenti in criptovalute. La dimensione emotiva rende questa truffa particolarmente difficile da riconoscere e da affrontare legalmente: le vittime spesso tardano a denunciare per vergogna o perché continuano a sperare che la relazione fosse autentica.

1.5 Lo Schema Ponzi in Criptovalute

I rendimenti promessi sono astronomici: dal 10 al 50% mensile, con sistemi di referral che remunerano chi porta nuovi investitori. Il sistema collassa inevitabilmente quando i nuovi ingressi non sono più sufficienti a pagare i rendimenti promessi. A quel punto i promotori spariscono con il capitale accumulato.

1.6 Il Rug Pull nella DeFi

Viene lanciato un nuovo token con grande clamore sui social media. Gli sviluppatori raccolgono ingenti somme in liquidità, poi improvvisamente ritirano tutti i fondi dal contratto intelligente e spariscono. Il token crolla a zero in pochi minuti, lasciando migliaia di investitori con asset privi di qualsiasi valore.

Capitolo 2

Le Nuove Frontiere della Frode: AI, Deepfake e NFT

Il panorama delle truffe crypto si evolve a velocità straordinaria. Nel 2024 e nel 2025 abbiamo assistito all'emergere di tipologie inedite che combinano l'intelligenza artificiale con i meccanismi classici della truffa finanziaria, con risultati devastanti.

2.1 I Deepfake di Personaggi Famosi

Attraverso software di intelligenza artificiale generativa, i truffatori creano video di alta qualità in cui personalità note — imprenditori, politici, personaggi dello spettacolo — promuovono fantomatiche piattaforme di investimento in criptovalute. La qualità dei video è spesso tale da rendere impossibile la distinzione a occhio nudo dal materiale autentico.

Regola fondamentale: nessuna persona famosa promuove piattaforme di investimento attraverso video sui social media. Se vedete un video del genere, si tratta sempre di una truffa. Senza eccezioni.

2.2 I Chatbot AI per la Manipolazione Personalizzata

Le organizzazioni criminali più sofisticate utilizzano oggi chatbot basati su modelli di linguaggio avanzati per condurre le prime fasi del Pig Butchering in modo completamente automatizzato. Questi sistemi sono in grado di sostenere conversazioni convincenti per settimane, costruendo un profilo psicologico dettagliato della vittima e adattando la strategia di manipolazione in tempo reale.

2.3 Le Truffe legate agli NFT

Il mercato degli NFT (Non-Fungible Token) ha generato nuove categorie di frode: la creazione di collezioni false con falsi artisti; il wash trading, ovvero transazioni circolari tra wallet controllati dallo stesso soggetto per gonfiare artificialmente il prezzo; i rug pull specifici per NFT, in cui gli sviluppatori abbandonano il progetto dopo aver venduto l'intera collezione.

2.4 Il Crypto Drainer

La vittima viene invitata a connettere il proprio wallet a un sito che promette NFT gratuiti o ricompense varie. Il sito contiene codice

malevolo — il cosiddetto “drainer” — che ottiene l’autorizzazione a svuotare automaticamente il wallet nel momento stesso della connessione. La peculiarità di questo attacco è che la vittima firma volontariamente una transazione, rendendo il recupero particolarmente complesso dal punto di vista legale.

Capitolo 3

Il Profilo Psicologico della Vittima e la Manipolazione Emotiva

Come è possibile che persone intelligenti cadano in queste truffe? La risposta richiede di abbandonare il pregiudizio secondo cui le vittime siano necessariamente ingenui o ignoranti. Le organizzazioni criminali specializzate impiegano psicologi, esperti di economia comportamentale e manipolatori professionisti.

3.1 I Sei Principi della Persuasione Applicati alla Frode

Robert Cialdini ha identificato sei principi fondamentali della persuasione. Tutti e sei vengono sistematicamente sfruttati nelle truffe crypto.

La reciprocità viene attivata attraverso i piccoli guadagni iniziali autorizzati: la vittima sente di dover qualcosa alla piattaforma. La scarsità si crea artificialmente attraverso offerte limitate nel tempo e investimenti presentati come riservati a pochi eletti. La prova sociale si costruisce con testimonianze false, screenshot di guadagni e community Telegram con migliaia di iscritti acquistati.

L'autorità si costruisce attraverso siti web professionali, finti regolatori internazionali e diplomi di certificazione falsi. La simpatia è il fondamento del romance scam: si crea prima un legame umano autentico, poi lo si strumentalizza. L'impegno e la coerenza operano quando la vittima ha già investito somme significative: rinunciare vorrebbe dire ammettere di aver sbagliato, e quindi si continua a versare denaro.

3.2 Il Ruolo della Vergogna nel Ritardo della Denuncia

Le vittime spesso attendono settimane o mesi prima di denunciare, paralizzate dalla vergogna. Questo ritardo è fatale: ogni ora che passa aumenta la probabilità che i fondi vengano spostati, convertiti o riciclati in modo definitivamente irrecoverabile.

La vergogna è l'arma più potente del truffatore. Nel corso dell'attività professionale ho incontrato medici, magistrati e professori universitari vittime di queste truffe. L'intelligenza non protegge dalla manipolazione emotiva: protegge l'informazione. L'unica risposta corretta è agire immediatamente.

PARTE SECONDA

LA SCIENZA DELLA BLOCKCHAIN

Come leggere il registro più trasparente della storia

Capitolo 4

La Trasparenza dell'Invisibile: Fondamenti di Chain Analysis Forense

La tecnologia Blockchain è il registro più pubblico della storia. Se inviate un bonifico bancario, solo le banche coinvolte vedono il flusso di denaro. Se inviate un Bitcoin, l'intera rete mondiale registra il passaggio in modo permanente e immutabile. Comprendere questa differenza fondamentale è la chiave per capire sia la vulnerabilità dei criminali sia le opportunità della difesa legale.

4.1 L'Impronta Digitale: Il TXID e gli Explorer

Ogni transazione sulla blockchain genera un Hash di transazione, comunemente noto come TXID (Transaction ID). È un codice alfanumerico univoco che identifica in modo permanente e irrevocabile: il wallet mittente, il wallet destinatario, l'orario esatto della transazione, l'importo trasferito e le commissioni pagate ai miner.

Questi dati sono pubblicamente consultabili attraverso i Block Explorer: strumenti web che permettono a chiunque di verificare qualsiasi transazione avvenuta su una determinata blockchain. I principali Block Explorer includono Blockchain.com per Bitcoin, Etherscan.io per Ethereum, Solscan.io per Solana e BscScan.com per BNB Chain.

Se la transazione non compare su nessun Block Explorer pubblico, la truffa è avvenuta esclusivamente a livello di database interno del sito fraudolento. I vostri fondi non sono mai entrati nella blockchain reale: sono stati semplicemente registrati su un database privato controllato dai criminali.

4.2 Tecniche di Layering, Clustering e Peeling Chains

Il truffatore professionista non mantiene i fondi sul primo wallet. Il Layering, o stratificazione, consiste in spostamenti rapidi tra decine o centinaia di wallet intermedi, effettuati in pochi minuti od ore, con l'obiettivo di confondere le tracce. Le Peeling Chains suddividono progressivamente un importo elevato: dieci Bitcoin diventano cento transazioni da 0,1 BTC inviate a indirizzi diversi.

Il Clustering è la risposta tecnica forense a queste strategie evasive. Attraverso software specializzati, è possibile identificare quali indirizzi, pur essendo apparentemente diversi e non collegati, appartengono alla

stessa entità criminale, analizzando i pattern di spesa comuni, i nodi di confluenza dei fondi e le caratteristiche tecniche delle firme crittografiche.

4.3 I Nodi di Uscita: I VASP e il Momento del Cash-out

Il tracciamento ha un obiettivo primario: individuare il VASP (Virtual Asset Service Provider), ovvero l'Exchange dove i fondi vengono depositati per essere convertiti in valuta tradizionale e prelevati dal sistema. Poiché questi soggetti sono legalmente obbligati a seguire le direttive KYC (Know Your Customer), è qui che l'identità digitale del truffatore incontra il mondo reale: un nome, un cognome e un documento d'identità verificato.

Capitolo 5

Gli Strumenti del Tracciamento Professionale

La Chain Analysis forense professionale si avvale di strumenti software specializzati che vanno ben oltre le capacità dei Block Explorer pubblici. Questi strumenti consentono di visualizzare graficamente i flussi di fondi, identificare cluster di indirizzi correlati e rilevare automaticamente pattern sospetti.

5.1 Chainalysis

Lo standard del settore, adottato da centinaia di agenzie governative in oltre settanta paesi. Chainalysis Reactor consente di tracciare graficamente i flussi attraverso reti complesse di indirizzi, identificare automaticamente i VASP di destinazione e generare report forensi conformi agli standard giudiziari. La sua forza risiede nel database proprietario che associa milioni di indirizzi blockchain a entità reali identificate: exchange, servizi illeciti, mixer e wallet personali.

5.2 Elliptic e TRM Labs

Elliptic eccelle nell'analisi degli asset DeFi e dei token ERC-20. TRM Labs si distingue per le capacità di analisi in tempo reale e per l'integrazione con sistemi di compliance aziendale. Entrambe le piattaforme vengono utilizzate per cross-verificare i risultati e garantire la solidità delle analisi forensi.

5.3 Strumenti Open Source per la Verifica Preliminare

Prima di investire nell'analisi professionale, è possibile effettuare verifiche preliminari attraverso strumenti gratuiti. Breadcrumbs.app offre funzionalità di tracciamento visuale per Bitcoin ed Ethereum. OXT.me è specializzato nell'analisi avanzata di Bitcoin. Maltego consente di costruire mappe di relazioni tra entità blockchain.

Capitolo 6

DeFi, Mixer e Privacy Coins: Quando il Tracciamento si Complica

Non tutti i casi di truffa crypto sono ugualmente tracciabili. Alcune tecnologie sono specificamente progettate per ostacolare il monitoraggio dei flussi finanziari, e i criminali più sofisticati le utilizzano sistematicamente.

6.1 I Crypto Mixer e i Tumbler

I mixer mescolano criptovalute di più utenti per spezzare il collegamento tra indirizzo mittente e indirizzo destinatario. Dal punto di vista tecnico, anche i mixer non sono impermeabili all'analisi forense: tecniche di taint analysis, analisi euristica e correlazione temporale permettono spesso di tracciare i fondi nonostante il mixing, specialmente quando i volumi trattati sono significativi.

6.2 Le Privacy Coins: Monero e Zcash

Monero (XMR) è la privacy coin per eccellenza. Utilizza tecnologie crittografiche avanzate — Ring Signatures, Stealth Addresses e RingCT — per rendere le transazioni opache per definizione. A differenza di Bitcoin, su Monero non è possibile determinare mittente, destinatario o importo di una transazione da un osservatore esterno. Il tracciamento di Monero è tecnicamente possibile solo con l'accesso diretto alle chiavi private del wallet.

6.3 La DeFi e i Bridge Cross-Chain

I Bridge cross-chain permettono di spostare asset da una blockchain all'altra, complicando il tracciamento. I protocolli di swap decentralizzati consentono di cambiare criptovaluta senza passare per un exchange con obblighi KYC. Nonostante queste complessità, i software forensi di ultima generazione hanno sviluppato capacità di analisi cross-chain che permettono di seguire i fondi attraverso la maggior parte di questi meccanismi.

PARTE TERZA

LA STRATEGIA LEGALE

Come trasformare i dati in azione penale concreta

Capitolo 7

La Querela Tecnico-Giuridica: Come Costruirla per Vincere

Possedere i dati di tracciamento blockchain è come avere le impronte digitali su una scena del crimine: sono inutili se non vengono presentate correttamente all'autorità giudiziaria tramite un legale esperto. La redazione della querela è il momento più critico dell'intera strategia legale.

7.1 Il Problema della Denuncia Generica

Il problema principale è la cosiddetta denuncia fotocopia. La vittima riferisce: "Ho investito su una piattaforma e non mi ridanno i soldi." Senza analisi tecnica allegata, questa denuncia finisce in fondo alla pila dei Magistrati con un alto rischio di archiviazione per ignoti. Il Pubblico Ministero non ha il tempo di effettuare analisi forense blockchain su ogni singolo caso: dobbiamo essere noi a fornirgli la prova già cristallizzata.

7.2 La Struttura della Querela Efficace

Una querela efficace per truffa in criptovalute deve contenere elementi tecnici e giuridici precisi. La sezione narrativa deve descrivere con precisione cronologica lo sviluppo della truffa, evitando elementi emotivi e concentrandosi sui fatti verificabili. La qualificazione giuridica deve identificare con esattezza i reati contestati. Il report forense allegato deve presentare l'analisi blockchain in formato comprensibile per il Magistrato, identificando il VASP di destinazione dei fondi.

7.3 La Corretta Qualificazione dei Reati

La scelta dei reati da contestare non è un dettaglio formale: è una scelta strategica che influenza radicalmente le possibilità di successo. La Truffa aggravata ai sensi dell'articolo 640, comma 2, c.p. è il reato più comunemente contestato. La Frode informatica ai sensi dell'articolo 640-ter c.p. è preferibile quando la truffa ha coinvolto specificamente sistemi informatici. L'Abusivismo finanziario ai sensi dell'articolo 166 TUF è applicabile quando la piattaforma offriva servizi di investimento senza le autorizzazioni di legge.

La corretta combinazione di reati è fondamentale per garantire la competenza della Procura più efficace, la possibilità di richiedere misure cautelari adeguate e i termini di prescrizione più favorevoli per la vittima.

Capitolo 8

Il Quadro Normativo: MiCA, D.Lgs. 231, TUF

8.1 Il Regolamento MiCA

Il Markets in Crypto-Assets Regulation (MiCA), entrato in vigore il 30 giugno 2024, rappresenta il primo quadro regolatorio completo per le criptovalute in Europa. Introduce l'obbligo di autorizzazione per tutti i CASP (Crypto-Asset Service Provider), crea obblighi stringenti di trasparenza e informativa, e stabilisce responsabilità civili e penali per le violazioni. Per le vittime di truffe, MiCA è rilevante perché consente di verificare immediatamente se la piattaforma era autorizzata.

8.2 Il D.Lgs. 231/2001

Il Decreto Legislativo 231/2001 introduce la responsabilità amministrativa degli enti per reati commessi nel loro interesse o vantaggio. Nei casi in cui una società italiana sia stata coinvolta, anche solo marginalmente, nell'operazione fraudolenta, questo decreto apre la possibilità di coinvolgere la persona giuridica nel procedimento penale.

8.3 Il Testo Unico della Finanza

Le piattaforme di trading fraudolente quasi invariabilmente violano il TUF, svolgendo attività riservate ai soggetti autorizzati senza le necessarie licenze. Questo è rilevante non solo per la querela penale, ma anche per eventuali azioni civili di risarcimento del danno nei confronti di soggetti che hanno facilitato l'operatività della piattaforma in Italia.

Capitolo 9

Giurisprudenza Rilevante: Le Sentenze Che Hanno Fatto Storia

9.1 Il Bitcoin come Bene Patrimoniale

La Corte di Cassazione ha progressivamente riconosciuto Bitcoin e le principali criptovalute come strumenti dotati di valore patrimoniale effettivo, equiparabili ai fini penali alla valuta tradizionale. Questo ha implicazioni fondamentali per la configurabilità del reato di truffa e per il calcolo del danno risarcibile.

9.2 Il Sequestro Preventivo di Criptovalute

Diverse pronunce di Tribunali italiani hanno ormai consolidato la possibilità di disporre il sequestro preventivo di criptovalute nell'ambito di procedimenti penali. La tecnica si applica sia ai wallet direttamente controllati dall'indagato sia ai saldi presso Exchange che abbiano ricevuto fondi di provenienza illecita.

9.3 La Confisca per Equivalente

Nei casi in cui il sequestro diretto non sia possibile perché i fondi sono stati già convertiti o riciclati, la giurisprudenza ha ammesso la confisca per equivalente: il sequestro di beni di valore equivalente alla somma sottratta, indipendentemente dalla loro natura. Questo amplia considerevolmente le possibilità di recupero anche nei casi più complessi.

Capitolo 10

Misure Cautelari e Sequestri d'Urgenza

Nelle truffe su criptovalute, il tempo è letteralmente denaro. Ogni ora che passa aumenta la probabilità che i fondi vengano spostati, convertiti o riciclati in modo definitivamente irrecuperabile. La capacità di agire con rapidità è la differenza tra il recupero e la perdita totale.

10.1 La Corsa contro il Tempo

La procedura ideale prevede il contatto con un legale specializzato entro quarantotto ore dalla scoperta della truffa, l'analisi forense urgente nelle prime ventiquattro ore di lavoro e la presentazione della querela con richiesta di sequestro nel minor tempo possibile.

10.2 Il Decreto di Sequestro Preventivo

Lo strumento principale è il Decreto di Sequestro Preventivo emesso dal Giudice per le Indagini Preliminari su richiesta del Pubblico Ministero. Consente di bloccare i fondi presso l'Exchange identificato, impedendo qualsiasi prelievo o movimento. Perché la richiesta venga accolta rapidamente, è essenziale che la querela contenga già l'analisi forense con l'identificazione precisa del VASP.

10.3 Il Congelamento Amministrativo Preventivo

In parallelo all'azione giudiziaria, è spesso possibile ottenere un congelamento amministrativo direttamente dall'Exchange attraverso l'invio di un Legal Notice documentato con l'analisi forense. Questo meccanismo può agire in poche ore, prima ancora che il procedimento giudiziario sia formalmente avviato. Il Legal Notice deve essere redatto in inglese, contenere l'analisi forense e una richiesta chiara di blocco del conto identificato.

PARTE QUARTA

IL CONFRONTO INTERNAZIONALE

Navigare i sistemi giudiziari di mezzo mondo

Capitolo 11

Gli Exchange e i Protocolli di Blocco

Individuare il wallet del truffatore è un successo tecnico. Congelare i fondi è un successo legale. Gli Exchange non sono nemici: sono soggetti regolati che, se approcciati correttamente, possono diventare alleati fondamentali nel recupero.

11.1 Il Legal Notice e il Canale per Avvocati

Gli Exchange di primo livello dispongono di dipartimenti legali dedicati, accessibili solo a professionisti. Attraverso il Legal Notice formale, documentato con l'analisi forense, si segnala all'Exchange che i fondi presenti su un determinato account sono provento di reato. La qualità della documentazione è determinante: un Legal Notice ben costruito ottiene risposte in poche ore.

11.2 I Livelli di Cooperazione

Non tutti gli Exchange cooperano con la stessa prontezza. Binance ha dimostrato una cooperazione significativa con le autorità europee. Coinbase, quotata in borsa negli Stati Uniti, ha i più alti standard di compliance al mondo. Kraken ha una reputazione consolidata per la cooperazione con le autorità giudiziarie europee.

Capitolo 12

OIE, Rogatorie e Cooperazione Internazionale

12.1 L'Ordine di Indagine Europeo

L'Ordine di Indagine Europeo (OIE) è lo strumento più potente per la cooperazione giudiziaria all'interno dell'Unione Europea. Consente alla Procura italiana di richiedere direttamente alle autorità di un altro Stato membro il compimento di atti di indagine, incluso il blocco e la confisca di asset digitali presso Exchange con sede in Europa. I tempi medi si misurano in settimane anziché in mesi.

12.2 Le Rogatorie Internazionali

Per i Paesi extra-UE, lo strumento è la rogatoria internazionale, formalmente denominata Mutual Legal Assistance Treaty (MLAT). I tempi sono più lunghi, ma per i Paesi con cui l'Italia ha accordi bilaterali solidi — come gli Stati Uniti, il Canada e la Svizzera — i risultati possono essere significativi.

12.3 Il Ruolo di Europol e Interpol

Nei casi di maggiore rilevanza è possibile attivare la cooperazione di Europol e Interpol. Europol dispone di unità specializzate in crimini finanziari digitali e ha condotto operazioni di grande successo contro organizzazioni criminali specializzate in truffe crypto.

Capitolo 13

Le Giurisdizioni Friendly e Quelle Ostili

13.1 Le Giurisdizioni Cooperative

Gli Stati Uniti sono la giurisdizione più cooperativa al mondo per i casi crypto. L'Unione Europea, grazie al framework MiCA e all'OIE, offre un ambiente sempre più favorevole. Giappone, Singapore e Australia hanno regolamentazioni avanzate e autorità di enforcement efficaci.

13.2 Le Giurisdizioni Problematiche

Alcuni Paesi dell'Asia meridionale e sud-orientale, dove molte organizzazioni di Pig Butchering hanno la propria base operativa, presentano sistemi giudiziari con capacità limitate in materia di crimini crypto. Per queste giurisdizioni, la strategia deve puntare sull'identificazione e il blocco dei fondi prima che raggiungano la destinazione finale.

PARTE QUINTA

CASI DI STUDIO E LEZIONI APPRESE

Dall'analisi della cronaca alla consapevolezza operativa

Capitolo 14

Casi di Studio Tratti dalla Cronaca: Analisi e Insegnamenti

I casi che seguono sono tratti da vicende di pubblico dominio, da sentenze pubblicate, da reportage giornalistici specializzati e da relazioni di organizzazioni internazionali anti-frode. Non si tratta di casi seguiti direttamente dall'autore, bensì di episodi analizzati e approfonditi a scopo didattico, per illustrare le dinamiche operative delle truffe crypto e le possibilità concrete di recupero. Tutti i dati riportati sono tratti da fonti pubbliche.

Caso A: Il Recupero tramite Exchange Cooperante (fonte: relazione Chainalysis 2023)

In un caso documentato da Chainalysis nel proprio rapporto annuale sulle frodi crypto, una vittima italiana aveva perso una somma significativa attraverso una piattaforma di falso trading con rendimenti garantiti. L'analisi blockchain successiva ha tracciato i fondi attraverso sette wallet intermedi verso un Exchange europeo con obblighi KYC.

Il Legal Notice inviato dallo studio legale che ha seguito il caso ha ottenuto il congelamento amministrativo del conto in poche ore. Il successivo decreto di sequestro preventivo ha consolidato il blocco. Una parte consistente della somma è stata restituita alla vittima attraverso la procedura giudiziaria.

Lezione operativa: l'identificazione tempestiva del VASP e l'invio immediato del Legal Notice sono la variabile più critica per il successo del recupero. Ogni ora di ritardo riduce le probabilità.

Caso B: L'Identificazione tramite Errore Operativo del Truffatore (fonte: Europol, 2022)

In un'operazione documentata da Europol, un'organizzazione criminale specializzata in Pig Butchering ha commesso un errore operativo critico: alcuni dei suoi operatori hanno effettuato accessi ai wallet di accumulo senza protezione VPN, rivelando indirizzi IP reali. L'analisi combinata dei dati blockchain e dei log di accesso agli Exchange ha consentito l'identificazione di più soggetti.

Parallelamente, una parte dei fondi era stata utilizzata per acquisti su piattaforme e-commerce con procedure KYC, fornendo ulteriori elementi

identificativi. L'operazione si è conclusa con diversi arresti e con il recupero parziale dei fondi per le vittime.

Lezione operativa: i truffatori commettono errori. La raccolta sistematica di tutti i dati tecnici disponibili — IP di connessione, pattern di accesso, indirizzi di destinazione — può rivelarsi determinante.

Caso C: I Limiti del Tracciamento con Privacy Coins (fonte: FATF Report 2023)

Il Financial Action Task Force ha documentato nel proprio rapporto 2023 casi in cui i truffatori hanno convertito i fondi illeciti in Monero attraverso exchange decentralizzati, rendendo il tracciamento definitivamente impossibile oltre un certo punto. Nonostante le analisi forensi approfondite e le richieste di cooperazione internazionale, solo una frazione minima dei fondi è stata recuperata.

Questi casi illustrano i limiti reali del tracciamento quando vengono utilizzate privacy coins combinate con protocolli DeFi. Il recupero è stato possibile solo per i fondi intercettati prima della conversione in Monero.

Lezione operativa: la velocità di azione è ancor più critica quando si sospetta l'utilizzo di privacy coins. Ogni ora di ritardo può rendere irreversibile la perdita.

Caso D: Il Romance Scam con Deepfake (fonte: FBI Internet Crime Complaint Center, 2024)

L'FBI ha documentato nel rapporto IC3 del 2024 un incremento significativo di romance scam in cui i truffatori utilizzavano video deepfake generati con intelligenza artificiale per simulare videochiamate autentiche con le vittime. In uno dei casi analizzati, una vittima aveva perso una somma ingente dopo mesi di relazione sentimentale online, durante la quale aveva effettuato numerose videochiamate con quello che credeva essere il proprio partner.

L'indagine successiva ha ricostruito che l'intera relazione era stata gestita attraverso software di deepfake in tempo reale. I fondi erano stati distribuiti su Exchange in tre diverse giurisdizioni. La cooperazione internazionale attivata ha consentito il recupero parziale.

Lezione operativa: la possibilità tecnica di simulare videochiamate reali attraverso deepfake ha reso il romance scam ancora più difficile da riconoscere. Nessuna videochiamata, per quanto convincente, può sostituire un incontro fisico verificato.

Capitolo 15

Gli Errori Più Comuni delle Vittime e Come Evitarli

15.1 L'Errore del Pagamento per lo Sblocco

Regola assoluta: non pagare mai, per nessun motivo, ulteriori somme per sbloccare fondi già versati su una piattaforma sospetta. Ogni pagamento aggiuntivo è denaro perso definitivamente.

15.2 Il Ritardo nella Denuncia

La vergogna è il principale ostacolo. Molte vittime attendono settimane o mesi prima di denunciare. Ogni giorno di ritardo riduce significativamente le possibilità di recupero.

15.3 La Denuncia Generica senza Analisi Tecnica

Una denuncia senza analisi blockchain allegata rischia di essere archiviata per mancanza di elementi investigativi concreti. È come denunciare un furto senza descrivere il ladro né fornire impronte digitali.

15.4 Il Recovery Scam: La Truffa nella Truffa

Dopo la perdita, molte vittime vengono ricontattate da falsi esperti di recupero crypto che promettono di hackerare la piattaforma e restituire i fondi in cambio di un pagamento anticipato. Si tratta invariabilmente di una seconda truffa, spesso organizzata dagli stessi criminali.

Nessun esperto legittimo di recupero crypto chiede pagamenti anticipati prima di aver ottenuto risultati concreti. Qualsiasi richiesta di questo tipo è una truffa.

15.5 La Distruzione Accidentale delle Prove

Cancellare le chat, chiudere l'account sulla piattaforma fraudolenta, eliminare le ricevute delle transazioni: tutti questi elementi sono fondamentali per la querela e per l'analisi forense. Prima di qualsiasi altra azione, è indispensabile cristallizzare le prove.

Conclusioni

Il Futuro della Giustizia Digitale

Le truffe crypto non sono una calamità ineluttabile. Sono crimini che lasciano tracce digitali indelebili. La sfida del futuro è la consapevolezza collettiva: non permettete che il panico o la vergogna vi immobilizzino dopo essere stati truffati.

Il panorama normativo è in rapida evoluzione in senso favorevole alle vittime. MiCA ha introdotto regole chiare per il settore europeo. Le autorità giudiziarie sviluppano competenze sempre più specifiche. Gli strumenti forensi diventano ogni anno più sofisticati. La cooperazione internazionale si consolida.

La blockchain è trasparente per chi sa leggerla. Il crimine digitale lascia tracce per chi sa trovarle. La giustizia digitale è possibile per chi sa come ottenerla.

Non aspettate. Ogni ora conta. Contattate immediatamente un legale specializzato.

Avv. Alessandro Santoro — Bologna, 2026

Appendice A — Checklist d’Emergenza

Se scoprite di essere stati vittime di una truffa crypto, seguite questi passi nell’ordine indicato:

1. STOP IMMEDIATO AI VERSAMENTI. Non pagare mai finti costi di sblocco, tasse AML o commissioni di qualsiasi tipo.
2. CRISTALLIZZATE LE PROVE. Fate screenshot di tutte le chat (Telegram, WhatsApp, email), della piattaforma con i saldi e di tutte le transazioni visibili.
3. ISOLATE I TXID. Conservate i codici univoci di tutte le transazioni crypto effettuate: sono fondamentali per l’analisi forense.
4. CONTATTATE LA VOSTRA BANCA. Segnalate le transazioni come fraudolente e richiedete il blocco di eventuali addebiti programmati.
5. NON CANCELLATE NULLA. Non chiudete account, non cancellate chat, non disinstallate app. Ogni elemento potrebbe essere una prova.
6. DIFFIDATE DEI RECOVERY SCAM. Chi vi contatta promettendo di recuperare i fondi in cambio di un pagamento sta tentando una seconda truffa.
7. CONTATTATE IMMEDIATAMENTE UN LEGALE SPECIALIZZATO. Non una denuncia generica: un avvocato esperto in crypto forensics che avvii subito l’analisi blockchain.
8. RICHIEDETE L’ANALISI FORENSE URGENTE. Ogni ora che passa riduce le probabilità di intercettare i fondi prima del cash-out definitivo.

Appendice B — Glossario Tecnico

AML (Anti-Money Laundering)

Insieme di norme e procedure finalizzate a prevenire il riciclaggio di denaro. Gli Exchange sono obbligati per legge a rispettare procedure AML stringenti.

Blockchain

Registro distribuito e immutabile che registra tutte le transazioni in modo permanente e pubblico. È la base tecnologica delle criptovalute.

CASP (Crypto-Asset Service Provider)

Categoria introdotta dal regolamento MiCA che include tutti i fornitori di servizi relativi alle crypto-attività, soggetti ad autorizzazione obbligatoria nell'UE.

Clustering

Tecnica di analisi forense che consente di identificare più indirizzi blockchain appartenenti alla stessa entità, sulla base di pattern comportamentali comuni.

Crypto Drainer

Software malevolo che, una volta autorizzato dalla vittima tramite la firma di una transazione, svuota automaticamente il wallet crypto.

DeFi (Decentralized Finance)

Ecosistema di servizi finanziari costruiti su blockchain senza intermediari centralizzati. La DeFi presenta sfide specifiche per il tracciamento forense.

KYC (Know Your Customer)

Procedura di verifica dell'identità dei clienti obbligatoria per gli Exchange regolamentati. È il punto di contatto fondamentale tra il crimine digitale e il mondo reale.

Layering

Tecnica di riciclaggio che consiste nel spostare fondi attraverso molteplici transazioni successive per oscurarne l'origine illecita.

MiCA (Markets in Crypto-Assets Regulation)

Regolamento europeo entrato in vigore nel 2024 che introduce un quadro normativo armonizzato per le cripto-attività nell'Unione Europea.

Mixer / Tumbler

Servizio che mescola criptovalute di più utenti per spezzare il collegamento tra indirizzo mittente e indirizzo destinatario.

NFT (Non-Fungible Token)

Token crittografico unico che certifica la proprietà di un asset digitale. Il mercato degli NFT ha generato nuove tipologie di truffe.

OIE (Ordine di Indagine Europeo)

Strumento di cooperazione giudiziaria europea che consente a una Procura di richiedere atti di indagine ad autorità di altri Stati membri.

Peeling Chain

Tecnica di offuscamento che consiste nel suddividere progressivamente un importo elevato in molte transazioni più piccole inviate a indirizzi diversi.

Pig Butchering

Tipologia di truffa in cui il criminale costruisce una relazione prolungata con la vittima prima di convincerla a investire su piattaforme fraudolente.

Rug Pull

Tipologia di truffa in cui gli sviluppatori di un progetto crypto ritirano improvvisamente tutta la liquidità, causando il crollo del valore del token a zero.

TXID (Transaction ID)

Identificativo univoco di ogni transazione sulla blockchain. È l'impronta digitale fondamentale per l'analisi forense.

VASP (Virtual Asset Service Provider)

Fornitore di servizi su asset virtuali, tipicamente un Exchange. I VASP sono il punto di uscita principale dei fondi illeciti verso la valuta tradizionale.

Appendice C — Normativa di Riferimento

Normativa Penale Italiana

- Art. 640 c.p. — Truffa
- Art. 640-ter c.p. — Frode informatica
- Art. 648-bis c.p. — Riciclaggio
- Art. 648-ter.1 c.p. — Autoriciclaggio

Normativa Finanziaria

- D.Lgs. 58/1998 (TUF) — in particolare art. 166 sull'abusivismo finanziario
- D.Lgs. 231/2001 — Responsabilità amministrativa degli enti
- D.Lgs. 231/2007 — Normativa antiriciclaggio

Normativa Europea

- Regolamento MiCA (EU) 2023/1114
- Direttiva (EU) 2018/843 — V Direttiva Antiriciclaggio
- Regolamento (EU) 2023/1113 — Transfer of Funds Regulation
- Direttiva (EU) 2014/41 — Ordine Europeo di Indagine Penale

Appendice D — Risorse Utili e Contatti

Studio Legale Santoro

- Indirizzo: Bologna, Piazza Galileo n. 5
- Tel: +39 051 621 5920
- Mobile: +39 328 684 1828
- Email: santoroalessandro22@gmail.com
- Web: www.avvocatosantorobologna.com

Autorità di Riferimento in Italia

- Polizia Postale e delle Comunicazioni: www.commissariatodips.it
- CONSOB — Commissione Nazionale per le Società e la Borsa: www.consob.it
- UIF — Unità di Informazione Finanziaria: www.uif.bancaditalia.it
- Banca d'Italia: www.bancaditalia.it

Strumenti di Verifica

- Blockchain.com — Block Explorer per Bitcoin
- Etherscan.io — Block Explorer per Ethereum
- Solscan.io — Block Explorer per Solana
- CONSOB — Registro dei soggetti autorizzati
- ESMA — European Securities and Markets Authority

Per Segnalare una Truffa

- Polizia Postale: www.commissariatodips.it/segnalazioni
- CONSOB — Segnalazioni: www.consob.it/web/area-pubblica/segnalazioni
- Europol: www.europol.europa.eu

L'AUTORE

L'Avv. Alessandro Santoro è un penalista con oltre 20 anni di esperienza, con sede a Bologna presso lo Studio Legale Santoro in Piazza Galileo n. 5. Si è specializzato nel diritto penale applicato alle tecnologie digitali e alle criptovalute, diventando uno dei principali riferimenti italiani per le vittime di truffe su Bitcoin e asset digitali.

È autore del libro "Il Futuro Legale delle Criptovalute (Smart Contract e Blockchain)", disponibile su Amazon, e gestisce il canale YouTube @AvvocatoSantorodirittopenale dedicato alla divulgazione del diritto penale delle criptovalute.

Assiste clienti in tutta Italia nelle fasi di querela, analisi forense blockchain, richieste di sequestro preventivo e costituzione di parte civile nei procedimenti per truffa su criptovalute.

www.avvocatosantorobologna.com

+39 328 684 1828