Crypto Scams 2025: come l’analisi forense blockchain combatte le frodi



Una delle espressioni che è balzata alle cronache recentemente è “crypto scams 2025”, simbolo di un fenomeno in crescita che ha bruciato miliardi di dollari tra truffe, hack e frodi d’investimento. L’articolo analizza come la tecnologia blockchain, nata per garantire trasparenza e decentralizzazione, stia diventando anche l’arma principale per smascherare la criminalità digitale, con l’Italia tra i protagonisti nella ricerca e nelle investigazioni forensi.

Nel 2024, gli americani hanno perso 16.6 miliardi di dollari a causa della criminalità informatica, di cui 9.3 miliardi direttamente legati alle criptovalute. Un paradosso singolare: le stesse tecnologie blockchain progettate per garantire privacy e decentralizzazione stanno diventando gli strumenti più potenti nelle mani degli investigatori digitali. La Prof. Laura Ricci dell’Università di Pisa lo spiega con efficacia: “La blockchain non è solo il registro delle transazioni Bitcoin, ma un vero e proprio notaio digitale che rende tracciabile ciò che i criminali credevano invisibile.”

Questa contraddizione apparente nasconde una verità più complessa. Mentre le truffe crypto continuano a crescere del 66% anno su anno secondo l’FBI Internet Crime Complaint Center, le forze dell’ordine stanno affinando tecniche investigative che sfruttano proprio l’immutabilità e la trasparenza delle blockchain pubbliche. Il risultato? Una corsa agli armamenti tecnologica dove ogni nuovo strumento di anonimizzazione trova la sua contromisura forense.

L’anatomia tecnica dell’investigazione blockchain: oltre il mito dell’anonimato

Quando Ross Ulbricht lanciò Silk Road nel 2011, credeva che l’anonimato di Tor combinato con i pagamenti in Bitcoin avrebbe creato un mercato nero invulnerabile. Non aveva fatto i conti con una realtà fondamentale: Bitcoin non offre anonimato, ma pseudo-anonimato. La differenza è abissale.

Ogni transazione Bitcoin lascia tracce indelebili sulla blockchain. Gli investigatori forensi utilizzano tecniche sofisticate di **address clustering** per collegare indirizzi apparentemente scollegati alla stessa entità. L’euristica più potente è la common input heuristic: quando più indirizzi Bitcoin vengono utilizzati come input nella stessa transazione, con alta probabilità appartengono allo stesso wallet o utente. Chainalysis, leader globale nell’analisi blockchain con oltre 100 euristiche proprietarie che monitorano 25+ blockchain, ha costruito il suo impero su questo principio.

Ma c’è di più. La **change address detection** permette di distinguere quali output di una transazione rappresentano il pagamento reale e quali sono il “resto” che torna al mittente. Tecniche di **graph analysis** trasformano la blockchain in una rete sociale dove algoritmi come PageRank identificano nodi centrali nelle reti criminali. La **taint analysis** traccia la “contaminazione” dei fondi attraverso catene di transazioni, quantificando matematicamente quanto denaro pulito si mescola con fondi illeciti.

Il Pisa Distributed Ledger Laboratory, guidato dalla Prof. Ricci con 3 membri permanenti, 2 post-doc e 6 dottorandi, ha contribuito significativamente a questa scienza emergente. Le loro ricerche sulla struttura “bow tie” del grafo degli utenti

Bitcoin hanno rivelato pattern comportamentali che distinguono attività legittime da schemi di riciclaggio. Quando i Carabinieri italiani, attraverso il Maggiore Simone Vecchiarello della Sezione Criptovalute del Comando Antifalsificazione Monetaria, applicano questi algoritmi sul campo, i risultati sono tangibili: operazioni che portano al sequestro di milioni in asset digitali.

L'epidemia delle investment fraud: 6.57 miliardi evaporati nel 2024 – il volto delle crypto scams 2025

Se dovessimo identificare il volto dominante della criminalità crypto nel 2024, sarebbe quello delle investment fraud. Con 6.57 miliardi di dollari persi secondo l'FBI IC3 Report, rappresentano il 40% di tutte le perdite legate a criptovalute. Non stiamo parlando di hack tecnici o exploit di smart contract, ma di ingegneria sociale applicata con precisione chirurgica.

Le truffe "pig butchering" meritano attenzione particolare per la loro sofisticazione psicologica. Il termine, traduzione letterale del cinese "sha zhu pan" (letteralmente "piatto di maiale macellato"), descrive una truffa in più fasi dove la vittima viene "ingrassata" con piccoli guadagni iniziali prima della "macellazione" finale. Il truffatore costruisce una relazione online, spesso romantica, che può durare settimane o mesi. Introduce gradualmente opportunità di investimento in criptovalute, mostrandosi esperto e condividendo screenshot di profitti apparentemente reali. Quando la vittima investe somme significative, i fondi spariscono e con loro il truffatore.

L'impatto demografico è devastante. Le vittime over-60 hanno perso 4.885 miliardi di dollari nel 2024, rappresentando il 52% delle perdite totali da investment fraud. Questi numeri raccontano una storia di vulnerabilità generazionale: una

popolazione cresciuta nell’era pre-digitale si confronta con truffe progettate da nativi digitali che sfruttano sofisticati bias cognitivi.

Hack da record: quando 1.5 miliardi evaporano in una notte

Febbraio 2025 ha segnato un punto di svolta nella storia della criminalità crypto. ByBit, uno dei maggiori exchange al mondo, ha subito il furto più grande della storia: 1.5 miliardi di dollari spariti in quella che l’FBI ha formalmente attribuito alla Corea del Nord attraverso una Public Service Announcement pubblicata il 26 febbraio 2025.

L’attacco dimostra l’evoluzione delle capacità offensive degli stati-nazione nel dominio crypto. Il gruppo Lazarus, braccio cyber del regime nordcoreano, ha mostrato una padronanza tecnica che combina social engineering avanzato, infiltrazione delle infrastrutture IT e conoscenza profonda dei protocolli blockchain. Secondo Chainalysis, al 31 luglio 2025 i furti totali hanno raggiunto 2.17 miliardi di dollari, con gli exchange che assorbono il 76.65% delle perdite.

Ma c’è un dettaglio che sfugge alle statistiche aggregate: il 23.35% dei furti ha colpito wallet personali, con 8.5 miliardi di dollari in crypto rubate ancora detenute on-chain. Questi “wrench attacks” rappresentano un’evoluzione inquietante del crimine crypto. Non servono più exploit zero-day o vulnerabilità dei smart contract: basta violenza fisica o minacce credibili per ottenere seed phrase e chiavi private. È il ritorno a forme di criminalità brutalmente tradizionali applicate a tecnologie ultramoderne.

Ransomware: il declino inaspettato

che spiega più di quanto sembri

Se c’è una statistica che sorprende nell’anno della crescita esponenziale delle truffe crypto, è questa: i pagamenti ransomware sono crollati del 35.82% nel 2024, scendendo a 813.55 milioni di dollari dai 1.25 miliardi dell’anno precedente. Chainalysis attribuisce questo declino a tre fattori convergenti: maggiore resilienza delle vittime che rifiutano di pagare, operazioni di law enforcement più efficaci contro le gang ransomware, e migliore cyber hygiene aziendale.

Ma questo apparente successo nasconde una realtà più complessa. Il numero di attacchi ransomware non è diminuito significativamente; è diminuito il tasso di successo dei pagamenti. Le aziende stanno imparando che pagare non garantisce il recupero dei dati e finanzia ulteriori attacchi. Le banche dati di backup offline stanno diventando standard, rendendo meno critico il pagamento del riscatto.

Contemporaneamente, le frodi ai crypto ATM sono esplose del 99% in termini di complaint (anche se le perdite monetarie sono aumentate del 31%), raggiungendo 246.7 milioni di dollari secondo l’FBI. Questo spostamento rivela un pattern: quando una modalità di attacco diventa meno profittevole, i criminali migrano rapidamente verso vettori alternativi. I crypto ATM offrono vantaggio cruciale: anonimato operativo e conversione immediata cash-to-crypto senza KYC rigoroso.

Silk Road, FTX e Bitfinex: lezioni magistrali di analisi forense

Alcuni casi studio trascendono la cronaca criminale per diventare manuali operativi dell’investigazione blockchain. Silk Road rimane l’archetipo: quando l’FBI arrestò Ross Ulbricht nell’ottobre 2013, sequestrando oltre 600,000 Bitcoin

(successivamente convertiti in oltre un miliardo di dollari), l'operazione combinò OSINT tradizionale e analisi blockchain pionieristica.

L'errore fatale di Ulbricht? Un post su un forum nel 2011 dove l'username "altoid" aveva promosso Silk Road indicando l'email "rossulbricht@gmail.com" per ulteriori informazioni. L'analisi forense blockchain fece il resto: tracciare commissioni attraverso migliaia di transazioni, identificare pattern di consolidamento nei wallet, correlare temporalmente depositi e prelievi. La lezione è chiara: l'anonimato è una catena, forte quanto il suo anello più debole.

FTX rappresenta il polo opposto dello spettro criminale. Non un mercato nero costruito sull'anonimato, ma una frode finanziaria da 8 miliardi di dollari perpetrata in piena luce, con l'apparenza di legittimità. Nansen Analytics ha tracciato 280 milioni di token FTT (80% del supply totale) controllati da entità FTX/Alameda, rivelando la manipolazione sistemica che sosteneva l'impero di Sam Bankman-Fried. Quando FTX è collassato, 477 milioni di dollari sono stati rubati in circostanze ancora poco chiare, con 74 milioni riciclati ironicamente attraverso RenBridge, un servizio controllato dalla stessa Alameda Research.

Ma è il caso Bitfinex che dimostra la pazienza metodica dell'analisi forense blockchain. Nel 2016, hacker sconosciuti rubarono 119,754 Bitcoin dall'exchange (circa 72 milioni di dollari all'epoca). Per cinque anni, gli investigatori hanno tracciato meticolosamente ogni movimento di questi fondi attraverso exchange, mixer e wallet. Nel febbraio 2022, l'FBI ha arrestato Ilya Lichtenstein e Heather Morgan, sequestrando 94,000 Bitcoin valutati 3.6 miliardi di dollari al momento del sequestro (oltre 10 miliardi ai prezzi attuali).

La tecnica chiave? Peeling chain analysis: seguire la "spellatura" sistematica di un grande wallet in porzioni sempre più piccole attraverso migliaia di transazioni. Ma il

breakthrough decisivo venne da errori operativi offline: acquisti con gift card Walmart pagati in Bitcoin tracciabili a conti personali. Ancora una volta, la lezione è che la blockchain forense funziona meglio quando combinata con investigazione tradizionale.

Italia in prima linea: ecosistema di eccellenza tra ricerca e law enforcement

L'Italia sta costruendo un ecosistema crypto forensics tra i più avanzati d'Europa, combinando ricerca accademica d'avanguardia, forze dell'ordine altamente specializzate e framework normativi progressivi. Questa sinergia multi-attore rappresenta un modello di riferimento internazionale.

Il Pisa Distributed Ledger Laboratory guida la ricerca accademica italiana. La Prof. Laura Ricci, coordinatrice del curriculum "Sistemi sociali e società smart" nel Dottorato Nazionale in Blockchain and Distributed Ledger Technologies ed ex membro del gruppo di esperti del Ministero dello Sviluppo Economico per la strategia nazionale blockchain (2018-2019), ha creato un laboratorio con 3 membri permanenti, 2 post-doc, 2 ricercatori CNR e 6 dottorandi. Le pubblicazioni su graph analysis, detection di comportamenti artificiali e clustering di indirizzi Bitcoin non restano confinate alle riviste peer-reviewed: diventano algoritmi operativi per le forze dell'ordine.

L'Osservatorio Blockchain & Web3 del Politecnico di Milano, nato nel 2018, rappresenta il polo di riferimento nazionale per l'analisi del mercato blockchain. Con la collaborazione tra il Dipartimento di Ingegneria Gestionale e il Dipartimento di Elettronica, Informazione e Bioingegneria, l'Osservatorio monitora 2,033 progetti globali dal 2016, quantificando il mercato italiano blockchain a 42 milioni di euro con crescita

del 50% annuale. Il Blockchain Innovation & Solutions HUB facilita ricerca applicata pre-competitiva tra aziende, università e istituzioni.

L'Università di Perugia ospita il Cybersecurity Lab diretto dal Prof. Stefano Bistarelli, vincitore del Microsoft Azure Research Award per il progetto "Data Science for investigating the block-chain in Bitcoin". Il laboratorio sviluppa tecniche per identificare indirizzi blockchain utilizzati per attività illecite, contribuendo alla formazione di "hacker etici" attraverso CyberChallenge.IT.

Sul fronte operativo, i Carabinieri hanno istituito strutture specializzate uniche in Europa. Il Maggiore Simone Vecchiarello guida la Sezione Criptovalute del Comando Carabinieri Antifalsificazione Monetaria, sviluppando script proprietari per la ricostruzione di seed phrase e tecniche avanzate di analisi on-chain che combinano Chainalysis Reactor con tool interni. L'operazione Franco Lee ha dimostrato queste capacità: smantellamento di una rete da 8.8 milioni di euro con sequestro di Bitcoin, USDT, Ethereum e Matic.

La Guardia di Finanza opera attraverso due nuclei specialistici d'eccellenza. Il Nucleo Speciale Tutela Privacy e Frodi Tecnologiche, con 5 gruppi investigativi dedicati, monitora costantemente Clear Web, Dark Web e Deep Web per individuare riciclaggio e finanziamento del terrorismo. Utilizza software avanzati di blockchain analysis per tracciare wallet anonimi e transazioni sospette. Il Nucleo Speciale Polizia Valutaria si concentra sul contrasto ai flussi finanziari illeciti, collaborando strettamente con il Nucleo Privacy per operazioni congiunte.

Le operazioni recenti testimoniano l'efficacia di questa specializzazione: sequestro di 11 milioni di euro in Bitcoin e Avalanche per evasione fiscale (prima operazione europea di questa portata), individuazione di un trader con cripto-attività per 270 milioni di euro, e sequestro di wallet da 9

milioni di dollari creato con documenti falsi e deepfake. La Guardia di Finanza ha redatto una “Guida Operativa sulle investigazioni tecnologiche” distribuita a tutti i reparti, e partecipa a master universitari presso le Università “Tor Vergata” e “La Sapienza” di Roma, creando un circolo virtuoso tra formazione e operatività.

La Polizia Postale e delle Comunicazioni ha gestito 54,554 fascicoli nel 2024, con truffe online che hanno sottratto 181 milioni di euro (+32% rispetto al 2023). Questi numeri raccontano pressione criminale crescente ma anche capacità investigativa in evoluzione, con cooperazione internazionale continua attraverso Europol, Interpol ed EPPO.

Il framework normativo completa l’ecosistema. L’implementazione del regolamento MiCAR attraverso il Decreto Legislativo 129/2024 ha creato supervisione condivisa tra Banca d’Italia e CONSOB, posizionando l’Italia tra i primi paesi europei con compliance piena alle direttive comunitarie. Questa rapidità normativa, combinata con eccellenza accademica e specializzazione operativa, trasforma l’Italia in un laboratorio dove innovazione tecnologica e legalità non sono antagonisti ma alleati strategici nella guerra globale contro la criminalità finanziaria digitale.

L’arsenale tecnologico: quando l’intelligenza artificiale incontra la blockchain

L’analisi forense blockchain del 2025 è irriconoscibile rispetto a quella di cinque anni fa. Le piattaforme professionali come Chainalysis Reactor non si limitano più a tracciare transazioni: utilizzano machine learning per predire comportamenti, identificare pattern anomali in tempo reale, e assegnare risk scores automatizzati a indirizzi e transazioni.

Elliptic, con il suo database di 6.4 miliardi di indirizzi etichettati su 43 reti blockchain, applica Graph Neural Networks (GNN) per migliorare l'accuratezza del clustering del 10-15% rispetto ai metodi tradizionali. Ma è nell'applicazione di algoritmi di ransomware detection che il machine learning mostra risultati impressionanti: modelli basati su Random Forest e XGBoost raggiungono F1-score tra 0.85 e 0.95, con picchi di accuratezza del 99.5% su dataset di transazioni Bitcoin correlate a ransomware.

La ricerca accademica sta esplorando frontiere ancora più avanzate. Graph Attention Networks (GAT) analizzano reti di transazioni con accuratezza superiore del 15% rispetto ai metodi classici, identificando anomalie comportamentali che sfuggono all'occhio umano e agli algoritmi tradizionali. Natural Language Processing applicato al monitoraggio del dark web correla menzioni di indirizzi crypto con coordinamento criminale, creando intelligence actionable in tempo reale.

Tuttavia, questa potenza computazionale solleva questioni etiche profonde. Quando sistemi di intelligenza artificiale possono tracciare ogni movimento finanziario di un individuo attraverso la blockchain, dove tracciamo il confine tra sicurezza e sorveglianza di massa? Il GDPR europeo introduce tensioni fondamentali: come garantire il "diritto all'oblio" su una tecnologia progettata per essere immutabile?

Privacy versus sicurezza: il dilemma irrisolto delle privacy coin

Monero rappresenta la risposta tecnologica più sofisticata al problema della privacy blockchain. Con ring signatures, stealth addresses e RingCT che oscurano mittente, destinatario e ammontare di ogni transazione, Monero rimane largamente intracciabile nonostante l'IRS abbia offerto 1.25 milioni di

dollari in contratti (625,000 dollari ciascuno a Chainalysis e Integra FEC) per sviluppare strumenti di tracciamento.

Il fallimento di questi sforzi non è tecnologico ma fondamentale: Monero è progettato con privacy-by-default a livello protocollare, non come funzione aggiuntiva. Zcash offre privacy attraverso zero-knowledge proofs (zk-SNARKs), ma la sua scelta di rendere le transazioni schermate opzionali lo rende vulnerabile: meno dell'1% delle transazioni sono fully shielded, creando un "anonymity set" troppo piccolo per garantire vera privacy.

Questo solleva domande scomode. Se tecnologie come Monero rendono impossibile il tracciamento, dovrebbero essere bandite? O il diritto alla privacy finanziaria è fondamentale in una società libera? Non esistono risposte semplici. I difensori della privacy citano diritti costituzionali e la necessità di proteggere dissidenti politici, whistleblower e cittadini in regimi autoritari. Gli investigatori sottolineano che la stessa tecnologia facilita terrorismo, traffico di esseri umani e pedopornografia.

Il futuro potrebbe risiedere in approcci intermedi. Zero-knowledge proofs permettono di provare proprietà di dati senza rivelare i dati stessi. È teoricamente possibile costruire sistemi dove un'autorità giudiziaria possa ottenere informazioni su transazioni specifiche attraverso meccanismi di "privacy selettiva", mantenendo anonimato per tutti gli altri. Ma implementare questi sistemi senza backdoor sfruttabili da attori malintenzionati rimane una sfida ingegneristica aperta.

La minaccia quantistica: quando la crittografia diventa obsoleta

Esiste una minaccia esistenziale che aleggia su tutta la crittografia moderna: il quantum computing. Gli algoritmi di

Shor, eseguiti su computer quantistici sufficientemente potenti, potrebbero rompere gli schemi di firma digitale ECDSA che proteggono Bitcoin ed Ethereum. Il consenso accademico e degli esperti NIST colloca questa minaccia in un orizzonte temporale di 10-15 anni.

Il problema non è ipotetico. Ogni transazione Bitcoin espone temporaneamente la chiave pubblica, che un quantum computer potrebbe teoricamente usare per derivare la chiave privata. Fondi in indirizzi "pay-to-public-key" non ancora spesi sono particolarmente vulnerabili. Si stima che tra 2 e 5 milioni di Bitcoin (valore attuale superiore a 200 miliardi di dollari) siano in indirizzi vulnerabili, molti appartenenti agli early adopter incluso Satoshi Nakamoto.

La comunità cripto è consapevole del rischio. Sono in sviluppo algoritmi di firma post-quantum come Lattice-based cryptography e Hash-based signatures. Ma la migrazione richiederà un hard fork coordinato delle principali blockchain, un processo politicamente complesso e tecnicamente rischioso. La finestra temporale è stretta: dobbiamo implementare crittografia post-quantum prima che computer quantistici sufficientemente potenti diventino disponibili, ma evitare migrazioni premature verso algoritmi non sufficientemente testati.

Prospettive future: tra regolamentazione e innovazione tecnologica

Il 2025 segna un punto di inflessione nella guerra contro la criminalità crypto. La regolamentazione MiCAR in Europa, l'implementazione italiana attraverso il Decreto Legislativo 129/2024 con supervisione di Banca d'Italia e CONSOB, e gli sforzi di armonizzazione normativa globale stanno creando un framework dove innovazione tecnologica e compliance non sono

antagonisti.

Le sfide rimangono monumentali. Le forze dell'ordine devono processare oltre 100 milioni di transazioni giornaliere attraverso blockchain multiple, identificando in tempo reale quelle sospette. La scarsità di dati di addestramento etichettati limita l'efficacia dei modelli di machine learning. Le tecniche criminali evolvono più rapidamente degli aggiornamenti dei modelli investigativi.

Ma emerge anche motivo di cauto ottimismo. La collaborazione tra accademia, industria e law enforcement sta dando frutti concreti. Centri di eccellenza come il Pisa Distributed Ledger Laboratory, l'Osservatorio Blockchain & Web3 del Politecnico di Milano, e il Cybersecurity Lab dell'Università di Perugia dimostrano che la ricerca può tradursi rapidamente in capacità operative. L'Italia, con la sua combinazione di eccellenza accademica e forze dell'ordine sempre più specializzate, si posiziona all'avanguardia di questa battaglia.

Il futuro della sicurezza blockchain dipenderà dalla nostra capacità di bilanciare tre imperativi apparentemente in conflitto: preservare l'innovazione tecnologica che rende le criptovalute rivoluzionarie, proteggere i diritti di privacy dei cittadini onesti, e fornire alle forze dell'ordine strumenti efficaci per combattere criminalità che non conosce confini. Non è un equilibrio facile da trovare, ma è l'unico percorso sostenibile per un futuro dove finanza decentralizzata e sicurezza possano coesistere.

La battaglia contro i crypto scams non è solo tecnologica, ma profondamente umana: richiede vigilanza, educazione, cooperazione internazionale e la volontà di adattare continuamente strumenti e strategie a un panorama criminale in costante evoluzione. I 16.6 miliardi di dollari persi nel 2024 non sono solo statistiche, ma vite devastate, risparmi evaporati, fiducia tradita. Ogni caso risolto, ogni milione recuperato, ogni rete criminale smantellata rappresenta non

solo una vittoria investigativa, ma un passo verso un ecosistema crypto più sicuro, più trasparente e più degno della fiducia che milioni di persone vi ripongono.

Fonti:

Federal Bureau of Investigation. (2025, May 12). FBI releases annual Internet Crime Report.

Federal Bureau of Investigation, Internet Crime Complaint Center. (2024). 2024 Internet Crime Report.

Federal Bureau of Investigation. (2025, February 26). North Korea responsible for $1.5 billion Bybit hack [Public Service Announcement PSA250226]. Internet Crime Complaint Center.

(2025). 2025 crypto crime trends from Chainalysis.

(2025, July). 2025 crypto crime mid-year update.

(2025, July 15). Italian Carabinieri leverage Chainalysis to dismantle illicit crypto exchange.

Repubblica Italiana, Gazzetta Ufficiale. (2024, September 13). Decreto legislativo 5 settembre 2024, n. 129: Attuazione del regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (MiCAR). Serie Generale n. 214.

Polizia di Stato. (2025, January 3). I dati delle attività della Postale nel 2024.

S. Department of Justice. (2020, November 5). United States files a civil action to forfeit cryptocurrency valued at over one billion U.S. dollars [Press release]. U.S. Attorney’s Office, Northern District of California.

S. Department of Justice. (2022, November 21). U.S. attorney announces historic $3.36 billion cryptocurrency seizure and conviction in connection with Silk Road dark web fraud [Press release]. U.S. Attorney’s Office, Southern District of New

York.

S. Department of Justice. (2022, February 8). Two arrested for alleged conspiracy to launder $4.5 billion in stolen cryptocurrency [Press release].

(2022). The $477 million FTX hack: Following the blockchain trail.

(2022). Blockchain analysis: The collapse of Alameda and FTX.

Ricci, L. (n.d.). Home page – Pisa Distributed Ledger Laboratory. Università di Pisa, Dipartimento di Informatica.

Ricci, L., Di Francesco Maesa, D., et al. (2017). Detecting artificial behaviours in the Bitcoin users graph. Online Social Networks and Media, 3-4, 63-74.

Loporchio, M., Di Francesco Maesa, D., Bernasconi, A., & Ricci, L. (2024). Skip index: Supporting efficient inter-block queries and query authentication on the blockchain. Future Generation Computing Systems.

(2024). Machine learning for blockchain data analysis: Progress and opportunities. arXiv:2404.18251v1.

Nature Scientific Reports. (2025). Graph convolution network for fraud detection in bitcoin transactions. Scientific Reports, 15, Article 95672.

Politecnico di Milano, School of Management. (2023). Osservatorio Blockchain & Web3: Blockchain & Web3 time to build. Osservatori Digital Innovation.

Politecnico di Milano. (2025, January 24). Blockchain & Web3 outlook 2024/25 [Convegno].

Il Sole 24 ORE. (2024, September 18). Vecchiarello (Carabinieri): “Cripto asset, così avviene il riciclaggio di denaro” [Video].

Il Messaggero. (2024, June 22). Franco Lee, arrestato a Roma l’influencer cinese che riciclava soldi in bitcoin. “Io sono un bancomat”.

(2025, January 3). Nel 2024 truffe online per 181 milioni di euro, aumento del 32%.

(2025, June 29). Criminali digitali, black market e criptovalute: L’Italia in prima linea nella guerra invisibile.

(2025, February 28). Criptovalute ed evasione fiscale: La Guardia di Finanza sequestra 11 milioni di euro.

Il Giorno. (2025, June 13). Sequestrato wallet con 9 milioni di euro in criptovalute: Dietro c’è un attacco hacker.

(2025, July 17). Crypto theft is booming as criminals increasingly turn to physical attacks.

(n.d.). Blockchain intelligence.

(n.d.). Crypto investigations solution.

(n.d.). Blockchain forensics: Elliptic Investigator.

(2024). Our new research: Enhancing blockchain analytics through AI.

Crystal Intelligence. (2025). FBI’s IC3 2024 annual Internet Crime Report says crypto fraud up 66%.

Tom’s Hardware. (2024, September 23). Crypto-asset: Opportunità e sfide per il sistema legale.

Fondazione Vittorio Occorsio. (2025, June 13). Criptovalute: Il contrasto agli usi illeciti – Corso FVO. Scuola di Perfezionamento delle Forze di Polizia.

Report Difesa. (2021, December 26). Guardia di Finanza: Il Nucleo Speciale Tutela Privacy e le frodi tecnologiche.

Dal Checco, P. (2023, January 19). Bitcoin forensics & blockchain intelligence – Il libro.

Monero Project. (n.d.). What is Monero (XMR)?

(2020). IRS dishes out $1.25 million for data firms to crack Monero.

Bitcoin News. (2020). Chainalysis and Integra win $1.25 million IRS contract to break Monero.

(n.d.). Zero-knowledge proof (ZKP) – Explained.

Palo Alto Networks. (n.d.). What is quantum computing’s threat to cybersecurity?

(n.d.). Bitcoin and quantum computing: Understanding the threats and building quantum resistance.

TRM Labs. (2025). A record-breaking year for cybercrime: Key findings from the FBI’s 2024 IC3 report.

(2025). 10 key numbers from the 2024 FBI IC3 report.

(2025). Crypto ransomware revenue drops 35% to $813 million in 2024 amid tougher crackdowns and victim resistance.

(2025). 2025 crypto crime mid-year report: Stolen funds surge to $2.17 billion.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/crypto-scams-2025/