Blockchain Forensics: oltre le criptovalute – tracciamento NFT e indagini DeFi



La blockchain forensics ha attraversato una trasformazione profonda negli ultimi anni. Se fino al 2020 l'analisi on-chain si concentrava principalmente sul tracciamento di Bitcoin ed Ethereum nelle indagini relative a darknet markets e ransomware, oggi gli investigatori digitali devono confrontarsi con un ecosistema infinitamente più complesso. La proliferazione dei Non-Fungible Token (NFT) e l'esplosione della finanza decentralizzata (DeFi) hanno trasformato la blockchain in un teatro dove si intrecciano frodi sofisticate, operazioni di riciclaggio multinazionale e crimini che sfidano le categorie giuridiche tradizionali.

L'evoluzione delle tecniche investigative richiede oggi competenze che vanno oltre la semplice analisi dei flussi transazionali. Come evidenziato nell'analisi blockchain per il tracciamento di criptovalute, gli investigatori devono padroneggiare tecniche di deanonimizzazione sempre più sofisticate per collegare indirizzi pseudo-anonimi alle identità reali degli attori coinvolti.

Il paradosso della trasparenza blockchain

Esiste un paradosso fondamentale nella blockchain forensics contemporanea: mentre la natura immutabile e trasparente del registro distribuito dovrebbe teoricamente rendere ogni transazione tracciabile all'infinito, la realtà operativa delle indagini su NFT e protocolli DeFi rivela una complessità che spesso vanifica questo assunto. La trasparenza della

blockchain non equivale automaticamente all'identificabilità degli attori, e questa distinzione è cruciale per comprendere le sfide investigative attuali.

Nel contesto degli NFT, il problema si manifesta con particolare evidenza. Un token non fungibile non è semplicemente un certificato digitale di proprietà: è un oggetto ibrido che vive simultaneamente on-chain e off-chain. La transazione registrata sulla blockchain documenta il trasferimento di un hash crittografico, ma l'asset effettivo – l'immagine, il video, il documento – risiede spesso su server IPFS, piattaforme cloud o server centralizzati controllati dal creatore. Questa biforcazione tra proprietà verificabile e controllo effettivo dell'asset crea zone grigie investigative che i tradizionali strumenti di blockchain analysis faticano a illuminare.

NFT Forensics – la complessità del tracciamento dei Token non fungibili

Metodologia investigativa stratificata

Il tracciamento di NFT richiede un approccio metodologico che integra analisi on-chain, intelligence off-chain e comprensione dei meccanismi economici sottostanti. A differenza delle criptovalute fungibili, dove l'analisi dei flussi transazionali può spesso risalire attraverso mixer fino a exchange centralizzati che applicano procedure KYC (Know Your Customer), gli NFT seguono percorsi di circolazione più erratici e meno prevedibili.

Un NFT può essere trasferito gratuitamente, venduto in una transazione peer-to-peer senza intermediari, depositato come collaterale in protocolli DeFi, frazionato attraverso processi di tokenizzazione, o persino "bruciato" in operazioni di

distruzione deliberata del token. Ogni passaggio lascia una traccia immutabile sulla blockchain, ma l'interpretazione investigativa di quella traccia richiede contesto specifico.

Wash Trading e manipolazione del mercato NFT

Consideriamo un caso investigativo emblematico: wash trading di NFT finalizzato a gonfiare artificialmente il valore di una collezione prima di una vendita fraudolenta. L'investigatore digitale può tracciare le transazioni on-chain, identificare pattern sospetti di compravendita tra wallet apparentemente diversi, ma stabilire la proprietà effettiva di quei wallet richiede un salto investigativo che esce dal perimetro della blockchain. Gli smart contract che governano i marketplace NFT registrano fedelmente ogni transazione, ma non possono attestare se i dieci wallet coinvolti in un meccanismo di price inflation appartengono alla stessa persona o entità.

Marketplace NFT e Punti di Convergenza Investigativa

Le piattaforme di marketplace come OpenSea, Blur o Rarible aggiungono un ulteriore livello di complessità. Quando un NFT viene venduto attraverso questi intermediari, la transazione on-chain registra l'interazione con lo smart contract del marketplace, non necessariamente l'identità economica dell'acquirente finale. Gli investigatori devono quindi integrare dati on-chain con log delle piattaforme, spesso accessibili solo attraverso richieste formali che richiedono cooperazione internazionale quando i server sono localizzati in giurisdizioni non collaborative.

Secondo il recente rapporto Eurojust-Europol 2024 sulla criminalità informatica, le frodi emergono come il reato più frequentemente associato all'utilizzo di NFT, mentre la finanza decentralizzata si afferma come nuovo territorio privilegiato per il riciclaggio di denaro criminale.

DeFi Investigations – il labirinto della finanza programmabile

Complessità investigativa dei protocolli decentralizzati

Se il tracciamento NFT presenta sfide significative, le indagini sui protocolli di finanza decentralizzata rappresentano un salto di complessità di ordine superiore. La DeFi non è semplicamente un'alternativa digitale alla finanza tradizionale: è un ecosistema di smart contract interconnessi dove capitale, rischio e governance sono programmati in codice e operano senza intermediari centralizzati.

Un'indagine tipica su una frode DeFi potrebbe iniziare con la segnalazione di un *rug pull* – la sottrazione improvvisa di liquidità da parte dei creatori di un protocollo. L'investigatore si trova immediatamente di fronte a una ragnatela di interazioni automatizzate: il protocollo fraudolento ha raccolto fondi attraverso un liquidity pool su Uniswap, i token emessi sono stati distribuiti attraverso meccanismi di yield farming, alcuni utenti hanno utilizzato quei token come collaterale su Aave o Compound, altri li hanno scambiati su aggregatori di exchange decentralizzati come 1inch.

Velocità di esecuzione e irreversibilità

Nel momento in cui i creatori eseguono la funzione di rug pull codificata nello smart contract, i fondi vengono trasferiti attraverso una cascata di transazioni che possono attraversare bridge cross-chain, protocolli di privacy, e infine approdare su exchange centralizzati dove vengono convertiti in valuta fiat. Ogni passaggio di questa catena è tecnicamente tracciabile, ma la velocità di esecuzione – spesso questione di minuti o addirittura blocchi – e la complessità delle interazioni rendono l'intervento investigativo in tempo reale

praticamente impossibile con gli strumenti attuali.

Frammentazione Cross-Chain e discontinuità investigative

Una caratteristica distintiva delle indagini DeFi è la frammentazione tra molteplici blockchain. L'ecosistema DeFi non vive più esclusivamente su Ethereum: protocolli significativi operano su Binance Smart Chain, Polygon, Avalanche, Solana, Arbitrum e decine di altre reti, ciascuna con le proprie caratteristiche tecniche, i propri explorer, e – crucialmente – i propri modelli di governance e compliance.

Questa frammentazione crea discontinuità investigative. Un'operazione di riciclaggio sofisticata può sfruttare bridge cross-chain per spostare valore tra blockchain diverse, trasformando ad esempio USDT su Ethereum in wrapped Bitcoin su Polygon, poi in token nativi su Avalanche, infine in stablecoin su Solana. Ogni passaggio attraverso un bridge rappresenta un punto di attrito investigativo dove la continuità del tracciamento richiede competenze tecniche specifiche e accesso a strumenti di analisi specializzati per ciascuna blockchain.

Vulnerabilità dei Bridge e zone grigie investigative

I bridge stessi rappresentano vettori di vulnerabilità non solo tecnica ma anche investigativa. Gli exploit su bridge – come il celebre attacco al Ronin Bridge che nel marzo 2022 ha sottratto circa 625 milioni di dollari, attribuito dal FBI al gruppo nordcoreano Lazarus – dimostrano come questi punti di interconnessione siano sia obiettivi prioritari per attaccanti sofisticati sia zone grigie dal punto di vista dell'attribuzione.

Come documentato nell'analisi dell'attacco Bybit del febbraio 2025, che ha visto la sottrazione di 1,5 miliardi di dollari

sempre da parte del gruppo Lazarus, anche i sistemi multi-firma considerati gold standard di sicurezza possono essere compromessi quando gli elementi chiave dell'infrastruttura operativa rimangono esposti a punti di fallimento centralizzati.

Smart Contract Forensics – decodificare l'intenzione dal codice

Analisi forense del codice come scena del crimine

Un aspetto distintivo delle indagini DeFi è la necessità di analizzare non solo le transazioni ma anche il codice degli smart contract che le hanno generate. Mentre nelle indagini su criptovalute tradizionali l'analisi si concentra sui flussi di valore, nelle indagini DeFi gli smart contract sono simultaneamente scena del crimine, strumento del reato e documentazione dell'attività illecita.

La forensics di smart contract richiede competenze che combinano analisi del codice, comprensione dei meccanismi economici e capacità di identificare pattern di vulnerabilità o funzionalità malevole deliberatamente nascoste. Un contratto che implementa un protocollo di lending apparentemente legittimo può contenere funzioni di "backdoor" che permettono ai creatori di drenare la liquidità in condizioni specifiche.

Tecniche di offuscamento e Reverse Engineering

Queste funzionalità possono essere mascherate attraverso tecniche di offuscamento del codice, distribuite tra contratti interconnessi, o attivabili solo attraverso combinazioni complesse di chiamate a funzioni. L'analisi forense deve quindi ricostruire non solo cosa è accaduto sulla blockchain,

ma cosa era progettato per accadere, quale intenzione era codificata nello smart contract. Questa dimensione dell'indagine richiede reverse engineering del codice Solidity o Vyper, comprensione dei pattern di design dei protocolli DeFi, e capacità di identificare deviazioni da standard consolidati che possono indicare intenti fraudolenti.

Quadro normativo europeo – MiCA e gli NFT

Markets in Crypto-Assets Regulation

Nel contesto europeo, il Regolamento MiCA (Markets in Crypto-Assets) rappresenta il primo tentativo organico di creare un framework normativo per crypto-asset. Entrato progressivamente in vigore – con le disposizioni su stablecoin (asset-referenced tokens ed e-money tokens) operative dal 30 giugno 2024 e piena applicazione dal 30 dicembre 2024 – MiCA stabilisce regole uniformi per emittenti e fornitori di servizi su crypto-asset in tutta l'Unione Europea.

L'ambiguità normativa degli NFT

MiCA esclude esplicitamente gli NFT "unici e non fungibili" dal proprio ambito di applicazione, ma la realtà del mercato NFT mostra che molti token presentano caratteristiche di fungibilità *de facto*: collezioni di migliaia di NFT con caratteristiche standardizzate vengono commerciati come asset speculativi più che come opere d'arte uniche. Questa ambiguità normativa si traduce in incertezza operativa per investigatori e autorità di law enforcement.

Obblighi antiriciclaggio e zone grigie

Quando un NFT viene utilizzato per riciclare denaro – uno scenario documentato in diversi casi investigativi, come analizzato nei risvolti penalistici delle criptovalute – quale

normativa antiriciclaggio si applica? Gli obblighi di segnalazione delle transazioni sospette gravano sui marketplace NFT? E quando questi marketplace sono piattaforme decentralizzate senza un'entità controllante identificabile, chi può essere oggetto di richieste investigative formali?

Protocolli di privacy e sanzioni – il caso Tornado Cash

Evoluzione normativa e giurisprudenziale

Il caso di Tornado Cash rappresenta un esempio emblematico delle sfide giuridiche e tecniche della blockchain forensics. Questo mixer di criptovalute basato su Ethereum fu sanzionato dall'Office of Foreign Assets Control (OFAC) statunitense nell'agosto 2022 per aver facilitato il riciclaggio di oltre 7 miliardi di dollari dal 2019, inclusi 455 milioni di dollari rubati dal gruppo Lazarus.

La vicenda ha preso una svolta significativa quando, nel novembre 2024, la Corte d'Appello del Quinto Circuito ha stabilito che gli smart contract immutabili di Tornado Cash non potevano essere classificati come "proprietà" ai sensi dell'International Emergency Economic Powers Act (IEEPA), in quanto privi delle caratteristiche di proprietà, controllo ed esclusività. Nel marzo 2025, l'amministrazione Trump ha rimosso le sanzioni su Tornado Cash, riconoscendo le "questioni legali e politiche innovative" sollevate dal caso.

Implicazioni per la Blockchain Forensics

Questa evoluzione normativa evidenzia come il riciclaggio attraverso protocolli di privacy decentralizzati continui a rappresentare una delle sfide più significative per gli investigatori digitali. Nonostante la rimozione delle sanzioni, le tecniche di chain hopping e l'utilizzo di servizi DeFi per convertire rapidamente asset tra diverse blockchain

rimangono strumenti privilegiati per organizzazioni criminali sofisticate.

Cooperazione internazionale e capacità investigative

Europol e l’European Cybercrime Centre

Organizzazioni come Europol, attraverso il suo European Cybercrime Centre (EC3) operativo dal 2013, hanno sviluppato unità specializzate per crimini legati alle criptovalute. Negli Stati Uniti, task force congiunte FBI-IRS si sono specializzate in crypto-crimes, conducendo indagini che hanno portato al sequestro di decine di milioni di dollari in asset illeciti.

Tuttavia, l’efficacia operativa rimane limitata dalla frammentazione normativa internazionale. Mentre alcuni paesi hanno sviluppato framework investigativi sofisticati, altre giurisdizioni mancano ancora delle competenze tecniche e del quadro normativo necessario per indagini efficaci su NFT e DeFi.

Arbitraggio giurisdizionale e strutture criminali

Il risultato è un panorama investigativo disomogeneo dove i criminali possono arbitraggiare tra giurisdizioni, sfruttando aree di debolezza normativa e tecnica. Protocolli DeFi possono essere strutturati deliberatamente per distribuire componenti critiche tra giurisdizioni diverse, rendendo interventi coordinati estremamente complessi dal punto di vista della cooperazione legale internazionale.

Forensics predittiva – intelligence

e prevenzione

Monitoraggio in tempo reale e machine learning

L’evoluzione della blockchain forensics sta progressivamente spostando il focus dalla ricostruzione post-factum verso l’intelligence preventiva. Sistemi di monitoraggio in tempo reale analizzano pattern transazionali su NFT e protocolli DeFi per identificare segnali di attività illecite in corso, permettendo interventi investigativi più tempestivi.

Algoritmi di machine learning vengono addestrati su dataset di frodi note per riconoscere pattern comportamentali sospetti: schemi di wash trading su NFT, movimenti di fondi che precedono rug pull in protocolli DeFi, indirizzi che mostrano comportamenti tipici di operazioni di riciclaggio.

Limiti strutturali dell’enforcement

Il limite di questi approcci è intrinseco alla natura aperta e permissionless della blockchain: mentre è possibile identificare comportamenti anomali, l’intervento preventivo rimane problematico in assenza di choke points centralizzati. Un exchange centralizzato può bloccare fondi sospetti su richiesta delle autorità; un protocollo DeFi decentralizzato non ha questa capacità strutturale.

L’enforcement deve quindi concentrarsi su punti di convergenza tra ecosistema decentralizzato e infrastruttura tradizionale: gli exchange che convertono crypto in fiat, i bridge verso blockchain più regolamentate, i marketplace NFT con politiche di compliance.

Prospettive future – competenze e coordinamento

Formazione tecnica continua come imperativo

La blockchain forensics applicata a NFT e DeFi non è una disciplina stabile ma un processo di adattamento continuo a un ecosistema tecnologico in rapida evoluzione. Ogni innovazione tecnologica – dai bridge cross-chain ai protocolli di privacy, dalle soluzioni Layer 2 ai meccanismi di governance decentralizzata – introduce nuove opportunità investigative ma anche nuove sfide.

Per i professionisti del diritto digitale, cybersecurity specialists e law enforcement, questo significa che la formazione tecnica continua non è opzionale. Comprendere come funziona un Automated Market Maker, cosa implica lo slippage in un DEX, come operano i protocolli di lending decentralizzati, non è cultura tecnica accessoria ma competenza investigativa fondamentale.

Il gap tra crimini e capacità investigative

Come evidenziato dal drammatico aumento delle crypto scam – con 9,3 miliardi di dollari persi nel solo 2024 secondo l'FBI e proiezioni che indicano 30 miliardi per il 2025 – l'alternativa è un'incapacità strutturale di comprendere e investigare crimini che operano nativamente in questi ecosistemi.

Verso un ecosistema investigativo integrato

La blockchain forensics del futuro sarà probabilmente meno dipendente dall'analisi post-factum e più orientata verso sistemi di intelligence continua, integrazione di dati on-

chain e off-chain, e sviluppo di capacità di intervento che anticipano piuttosto che reagire alle attività illecite.

Ma questo futuro richiede investimenti significativi in competenze, strumenti e soprattutto coordinamento internazionale che oggi appare ancora inadeguato rispetto alla portata e alla sofisticazione dei crimini che si manifestano nell'ecosistema blockchain contemporaneo. Solo attraverso un approccio multidisciplinare che unisce expertise tecnica, giuridica e investigativa sarà possibile costruire un framework efficace per contrastare le minacce emergenti nella frontiera digitale della finanza decentralizzata.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/blockchain-forensics/