AML Typologies Toolkit: Crypto Money Laundering Techniques & Detection Strategies

DAI Toolkit

Byline: DAI Research Desk · June 2026

Executive Summary

Criminal actors have refined sophisticated money laundering typologies exploiting blockchain infrastructure, cross-chain bridges, and DeFi protocols to obfuscate illicit fund flows. This toolkit catalogs eight high-priority AML typologies observed by law enforcement and compliance teams: mixing services (Tornado Cash, Sinbad.io), chain-hopping across multiple blockchains, exploitation of cross-chain bridges, over-the-counter (OTC) desk laundering, DPRK Lazarus Group operational patterns, ransomware payment laundering, darknet market cash-out mechanisms, and NFT wash trading for value transfer. Each typology presents distinct red flags, transaction patterns, and detection challenges. Compliance officers must implement layered surveillance combining on-chain analytics, behavioral monitoring, and cross-jurisdictional intelligence sharing to identify and report suspicious activity effectively. This briefing provides transaction-level indicators, case study patterns from FinCEN advisories and OFAC designations, and recommended detection parameters for transaction monitoring systems.

Background

Money laundering through cryptocurrency has evolved from rudimentary Bitcoin tumbling services circa 2013–2017 to sophisticated multi-stage operations leveraging DeFi protocols, privacy-enhancing technologies, and cross-chain infrastructure. The U.S. Department of Treasury's 2022 National Money Laundering Risk Assessment identified virtual assets as a "high-risk" vector for illicit finance, noting layering techniques that exploit blockchain pseudonymity, jurisdictional fragmentation, and rapid technological innovation.

By 2026, law enforcement agencies including FinCEN, FBI, IRS Criminal Investigation, Europol's European Cybercrime Centre (EC3), and specialized units in Singapore, UAE, and UK have documented hundreds of laundering schemes totaling billions in illicit proceeds. The Financial Action Task Force (FATF) updated its Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (October 2021, continuously referenced) emphasizing enhanced due diligence for high-risk transaction patterns including mixing, rapid movement across chains, and use of anonymity-enhancing technologies.

This toolkit draws on FinCEN advisories (FIN-2019-A003 on ransomware, FIN-2022-A004 on mixers), OFAC sanctions designations (Tornado Cash SDN August 2022, Sinbad.io designation November 2023), Chainalysis and TRM Labs public reporting, and FBI/DOJ indictments to catalog observable typologies and red flags.

Current Landscape (2026)

Mixing Services: Following OFAC's designation of Tornado Cash smart contracts in August 2022 and subsequent criminal prosecution of developer Alexey Pertsev (convicted in Netherlands, May 2024), the mixing landscape fragmented. Sinbad.io emerged as a successor service before its OFAC designation in November 2023. As of mid-2026, decentralized mixing protocols on newer chains (zkSync Era, Starknet, Aztec Network) and cross-chain privacy routers present evolving challenges. Chainalysis estimates ~$2.3 billion transited through sanctioned mixers in 2023–2024 pre-designation.

Chain-Hopping & Bridges: Cross-chain bridges (Multichain, Stargate, LayerZero-based protocols) enable rapid movement between Ethereum, BNB Chain, Polygon, Avalanche, Solana, and newer ecosystems. Criminals exploit bridge latency and chain-specific surveillance gaps. UNVERIFIED estimate: 40–60% of large-scale laundering operations (>$1M) incorporate at least one bridge hop by 2026.

OTC Desks: Over-the-counter brokers operating in jurisdictions with weak AML enforcement (UNVERIFIED: certain operators in Russia, parts of Southeast Asia, West Africa) facilitate direct fiat conversion without KYC. FinCEN's 2023 Advisory on Convertible Virtual Currency Mixing highlighted OTC desks as critical nexus points.

DPRK Activity: North Korea's Reconnaissance General Bureau (RGB), including Lazarus Group, Bluenoroff, and Andariel units, have stolen an estimated $3+ billion in cryptocurrency since 2017 (per UN Panel of Experts reports S/2023/171). Signature techniques include supply chain compromises, spear-phishing, exploit-driven heists (Ronin Bridge March 2022: $625M; Atomic Wallet June 2023: $100M), followed by methodical laundering via mixers, peel chains, and OTC conversion.

Ransomware: Ransomware payments continue flowing primarily to Bitcoin and Monero addresses. FinCEN reported ~$1.2 billion in suspected ransomware payments 2021–2023. Post-payment laundering involves immediate splitting to hundreds of addresses, mixer routing (pre-sanctions), and conversion via nested exchanges or P2P platforms.

Darknet Markets: Following takedowns of Hydra (April 2022, Germany BKA operation), AlphaBay reboot, and others, market operators and vendors launder proceeds via: (1) direct withdrawal to mixers, (2) exchange to privacy coins (Monero, Zcash shielded pools), (3) BTC → XMR → BTC round-tripping, (4) cash-out through P2P networks or complicit MSBs.

NFT Wash Trading: Beyond market manipulation, NFTs serve as value transfer vehicles—self-trading between controlled wallets to simulate legitimate provenance, followed by sale to unaffiliated buyer, converting dirty crypto into "clean" proceeds from ostensibly legitimate NFT sale. UNVERIFIED: relatively low volume (<$50M annually) but emerging.

Typology Breakdown & Red Flags

1. Mixing Services (Tornado Cash / Sinbad.io)

Mechanism: Users deposit cryptocurrency into a smart contract pool (Tornado Cash) or centralized custodial mixer (Sinbad), which aggregates funds and allows withdrawal to fresh addresses after delay, severing on-chain link between deposit and withdrawal addresses.

Red Flags:

- Direct deposit to or withdrawal from OFAC-sanctioned addresses (Tornado Cash: 0x… contracts listed on OFAC SDN).

• Repeated fixed-denomination deposits (0.1, 1, 10, 100 ETH) characteristic of Tornado Cash's anonymity set design.

• Withdrawal timing patterns: deposits followed by withdrawals 24–72 hours later to previously inactive addresses.

• Use of "relayers" (intermediary contracts that pay gas fees on behalf of withdrawal address to avoid linking funding transaction).

Detection Parameters:

• Flag any transaction interacting with SDN-listed contract addresses.

• Monitor for deposit/withdrawal pairs in fixed increments.

• Trace outputs from mixer withdrawals over subsequent hops (often immediate split to 10+ addresses).

Case Reference: Tornado Cash sanctions (OFAC August 8, 2022). Roman Storm and Roman Semenov indicted August 2023 (SDNY 23-CR-491) for conspiring to operate unlicensed money transmitting business and sanctions violations. Alexey Pertsev convicted Netherlands May 2024 (The Hague District Court) for facilitating money laundering.

2. Chain-Hopping

Mechanism: Moving funds across multiple blockchains (Ethereum → BNB Chain → Avalanche → Solana) to exploit surveillance gaps, jurisdictional differences in VASP compliance, and differing AML maturity of chain-native analytics.

Red Flags:

• Rapid sequential bridging (funds cross 3+ chains within 24 hours).

• Use of bridges shortly after identified illicit event (exchange hack, ransomware payment).

• Final destination chain hosted in jurisdiction with weak AML enforcement or no Travel Rule compliance (UNVERIFIED: some Tier 2/3 blockchains).

Detection Parameters:

• Integrate cross-chain transaction tracing tools (TRM, Chainalysis multi-chain, Elliptic).

• Monitor bridge contract interactions for high-velocity, high-value movements.

• Correlate bridge events with known compromise timestamps.

Case Reference: Ronin Bridge Hack (March 2022, Lazarus attribution by FBI). Stolen ETH bridged to Ethereum, immediately swapped and moved across Tornado Cash, then hopped to other chains for dispersion.

3. Cross-Chain Bridges Exploitation

Mechanism: Bridges themselves targeted as vulnerability points (smart contract exploits) and as laundering infrastructure. Post-exploit, attackers often bridge stolen funds multiple times to complicate tracing.

Red Flags:

• Transactions immediately following bridge security incident.

- Large inflows to bridge followed by immediate outflows to mixers or high-risk exchanges.
- Use of lesser-known or unaudited bridge protocols.

Detection Parameters:

- Subscribe to bridge exploit alert feeds (Blockchain Security Firms: CertiK, Peckshield, SlowMist).
- Cross-reference bridge user addresses with threat intelligence databases.
- Elevated scrutiny for transactions >$100K crossing bridges to chains with weak regulatory oversight.

Case Reference: Multichain bridge (formerly Anyswap) anomalies mid-2023 leading to $126M unexplained outflows. Funds traced through Ethereum and BNB Chain to various OTC desks (per TRM Labs).

4. OTC Desk Laundering

Mechanism: High-net-worth criminals or organizations arrange off-market cryptocurrency-to-fiat trades with brokers who either willfully ignore KYC or operate in non-cooperative jurisdictions. Provides liquidity without blockchain record of final fiat beneficiary.

Red Flags:

- Customer avoids on-exchange trading despite available liquidity.
- Requests for large-sum settlement in cash or offshore bank accounts.
- Counterparty OTC desk lacks regulatory registration or operates from high-risk jurisdiction per FATF lists.
- Funds sourced from mixers, darknet wallets, or ransomware-linked addresses.

Detection Parameters:

- For VASPs: require attestation and verification of OTC counterparty AML program.
- Enhanced due diligence on customers engaging OTC desks in Russia, certain CIS states, parts of MENA not aligned with FATF (UNVERIFIED specific jurisdictions; assess via FATF grey/blacklists).
- Monitoring for customer wallet interactions with known OTC addresses (public repositories: Chainalysis KYT, TRM risk scoring).

Case Reference: UNVERIFIED specific indictment linking OTC desk; FinCEN 314(b) sharing indicates pattern. Anecdotal intelligence from UK NCA (National Crime Agency) reports on OTC facilitators in Turkey and UAE facilitating GBP laundering.

5. DPRK Lazarus Patterns

Mechanism: DPRK-linked APT groups conduct sophisticated heists, followed by staged laundering: immediate dispersion to hundreds of addresses, batched mixer usage, conversion to Bitcoin or stablecoins, OTC cash-out, often via Chinese OTC brokers (per U.S. DOJ press releases).

Red Flags (Behavioral):

- Funds originating from known Lazarus-linked breach (FBI Flash Alerts, CISA advisories).
- Peel chain pattern: sequential transfers shedding small amounts to different addresses, retaining majority in "peeling" wallet.

- Mixing 7–14 days post-theft (delayed laundering to evade immediate surveillance).
- Conversion to BTC, then to emerging privacy chains or privacy-enhanced Bitcoin wallets (CoinJoin via Wasabi Wallet, Samourai pre-shutdown).
- Geographic cash-out indicators: OTC desks with China +86 Telegram contacts, settlement via Alipay/WeChat (per FBI advisories).

Detection Parameters:

- Real-time monitoring of FBI Cyber Division alerts and OFAC SDN updates.
- Cross-reference deposit addresses with DPRK attribution lists (maintained by Chainalysis, TRM, Elliptic).
- Enhanced scrutiny on peel chains: ≥50 sequential transfers with logarithmic decay.

Case Reference: FBI attribution Lazarus Group to Ronin (March 2022), Harmony Horizon Bridge (June 2022, $100M), Atomic Wallet (June 2023). DOJ indictment of Chinese nationals facilitating Lazarus laundering (U.S. v. Jiadong Li et al., May 2024, money laundering conspiracy).

6. Ransomware Payment Laundering

Mechanism: Victim pays ransom to attacker-controlled BTC/Monero address. Attacker immediately splits funds across dozens/hundreds of wallets, routes portions through mixers (pre-sanctions) or swaps to Monero, consolidates into larger wallets after several hops, then cashes out via nested exchanges or OTC.

Red Flags:

- Receipt from known ransomware payment address (cross-reference FinCEN, IC3, Chainalysis Ransomware Identification Dataset).
- Immediate splitting into 20–200 outputs within 1 hour of receipt.
- Rapid sequence: BTC → Exchange A (no KYC) → XMR → Exchange B → Fiat.
- Deposit to exchange from address ≤3 hops from identified ransomware wallet.

Detection Parameters:

- Implement ransomware address screening at deposit (block or flag for manual review).
- Velocity rules: ≥10 outbound transfers within 60 minutes.
- Monitor for BTC-to-privacy coin swaps ≥$10K on decentralized exchanges (Bisq, AtomicDEX).

Case Reference: FinCEN Advisory FIN-2019-A003 (October 2019, updated 2021) on ransomware trends. Colonial Pipeline ransom (May 2021, ~$4.4M BTC paid, ~$2.3M recovered by FBI via private key seizure). DarkSide/BlackMatter operations traced through multiple mixers and exchanges (Chainalysis 2022 Crypto Crime Report).

7. Darknet Market Cash-Out

Mechanism: Vendors accumulate cryptocurrency in market escrow or direct finalization wallets. Cash-out pathways: (1) Withdraw to personal wallet → swap BTC to XMR via decentralized exchange → withdraw XMR to offline wallet → sell XMR via P2P or non-compliant exchange. (2) Withdraw → mixer → exchange deposit via intermediary wallets → fiat withdrawal. (3) Consolidate and sell directly via OTC broker.

Red Flags:

- Deposits originating from known darknet market addresses (post-takedown law enforcement disclosures: Hydra wallet clusters, AlphaBay legacy addresses).
- Transaction graph shows convergence from multiple small inputs (consistent with vendor aggregating escrow releases).
- Immediate post-deposit conversion to Monero or privacy coin on integrated exchange (e.g., Binance BTC/XMR pair, if still available; or KuCoin, Gate.io).
- Withdrawal shortly after deposit to non-custodial wallet, indicative of pass-through.

Detection Parameters:

- Screen against darknet market address lists (updated post-takedown by Europol, DOJ).
- Behavioral: flag customers with frequent BTC → XMR → fiat pattern.
- Source of funds inquiries for customers depositing from addresses ≤2 hops from known market wallets.

Case Reference: Hydra Market takedown (April 2022, Germany/U.S. operation, servers seized). Post-seizure blockchain analysis identified vendor cash-out routes via Garantex (sanctioned exchange, OFAC April 2022) and other Russian-linked VASPs. DOJ Operation DisrupTor (September 2020) netted 179 arrests, identified common laundering via Localbitcoins P2P and mixers.

8. NFT Wash Trading & Value Transfer

Mechanism: (1) Wash trading: Attacker controls Wallet A (dirty funds) and Wallet B (clean). Wallet A mints or buys NFT, Wallet A "sells" NFT to Wallet B at inflated price, transferring value. Wallet B resells to third party, legitimizing funds. (2) Value parking: Purchase high-value NFT with illicit funds, hold, later sell for fiat/clean crypto.

Red Flags:

- Repeated transactions between same two wallets for same or similar NFTs.
- NFT sale prices significantly above floor/market (>200% deviation).
- Buyer wallet funded directly from mixer or high-risk source.
- Seller wallet immediately bridges or swaps proceeds post-sale, rather than holding.
- Self-trading pattern: Wallet A → Wallet B → Wallet A in circular trades.

Detection Parameters:

- Graph analysis: identify closed-loop trading (A ↔ B ↔ C ↔ A within 30 days).
- Price anomaly detection: flag sales >3 standard deviations from collection floor.
- Source of funds check: trace NFT purchase funding to deposit origin (mixer flag = high risk).

Case Reference: UNVERIFIED large-scale law enforcement case. However, U.S. Treasury National Risk Assessments (2022, 2024)