Virtual Currencies & Virtual Assets: How They're Abused for Money Laundering & Terrorist Financing

3-Day Training TOC

Prerequisites: Basic understanding of AML/CTF; familiarity with transaction data analysis (Excel/IDEA); laptop with internet access.
Learning outcomes (after 3 days):

- **Recognize major typologies for laundering & TF using crypto/virtual assets (VC/VA)**
- **Map blockchain transaction flows and identify red flags using open tools & CAATs (IDEA + graph tools)**
- **Understand key controls (VASP/KYC, Travel Rule, sanctions screening) and investigative steps**
- **Produce an intelligence brief / STR based on crypto evidence**

Day 1 — Foundations & Typologies (Theory + Demonstrations)

Duration: 6–7 hours (split into 4 sessions)

Session 1 — Intro to Virtual Currencies & Virtual Assets (60–75 min)

- What is a blockchain? Key concepts: public vs private ledgers, addresses, keys, wallets, transactions, blocks, confirmations.
- Types of virtual assets: cryptocurrencies (BTC, ETH), stablecoins, tokenized assets, NFTs, privacy coins (Monero), wrapped tokens, DeFi primitives (DEX, bridges, pools).
- Differences between custodial vs non-custodial wallets; centralised exchanges (CEX) vs decentralised exchanges (DEX).
- Quick demo: follow a single BTC transaction using a blockchain explorer (public demo on screen).

Learning objective: Understand where traceability exists and where it breaks.

Session 2 — How VC/VA are used in ML & TF (90 min)

- Typologies & phases mapped to AML lifecycle:
  - Placement: fiat-to-crypto on-ramps (P2P OTC, kiosks).
  - Layering: mixers/tumblers, CoinJoin, chain hopping, DEX swaps, cross-chain bridges, OTC brokers, privacy coins, mixers via tumblers.
  - Integration: cashing out via CEX, prepaid cards, merchant payments, NFTs, real estate.
- TF-specific typologies: small value transfers, splitting into micro-transactions, donation funnels (fraudulent charities), use of gaming platforms.
- Red flags: rapid chain hopping, use of sanctioned addresses, mixing services, newly created wallets tied to multiple cash-in points, spike in on-chain activity after cash deposits.

Case example (theory): How an illicit actor might use an OTC desk → mixer → stablecoin → bridge → CEX withdrawal.

Session 3 — Regulatory & Legal Landscape (60 min)

- VASP concept & why FATF matters (Travel Rule basics, KYC/CDD expectations for VASPs).
- Sanctions screening & designated addresses (OFAC/UN lists — how they apply to addresses and tools).
- Reporting obligations for STRs involving crypto, preservation of chain data, and evidence handling.
- Issues for cross-border cooperation (jurisdictional complexity, mutual legal assistance).

Practical tip: How to preserve chain evidence (export transactions, snapshot blocks, exchange preservation requests).

Session 4 — Demo: Tools of the Trade (60 min)

- Public blockchain explorers (Etherscan, Blockchair, Blockchain.info) — what you can extract.
- Open-source analytics & investigation tools: GraphSense/OXT/BlockSci (intro), address clustering basics.
- Commercial products (overview): Chainalysis, Elliptic, TRM — what they provide (alerting, clustering, sankey/graph views).
- Demo: Exporting ERC-20 transactions CSV from Etherscan; quick import into Excel/IDEA.

Hands-on mini exercise: Export 1 wallet's transactions (provided sample) and identify top incoming/outgoing counterparties.

Day 2 — Hands-on Chain Analysis & CAAT Integration

Duration: 6–7 hours (labs + guided exercises)

Session 1 — Data Extraction & Normalization (60–75 min)

- Where to get on-chain data: explorers, node RPC/JSON APIs, exchange ad-hoc disclosures (preservation).
- Export formats: CSV of transactions, token transfers, internal txns; mapping fields (txid, from, to, value, timestamp).
- Demonstration: Create a cleaned transaction dataset ready for IDEA/CAAT analysis.

Lab 1: Participants download a prepared sample CSV (simulated/anonymized) and import into Caseware IDEA (or Excel/ACL/CLOT).

Session 2 — Using IDEA / CAATs for Crypto Pattern Detection (90 min)

- Common CAAT queries for crypto data:
  - Gap detection: large time gaps between deposits/withdrawals vs. expected payroll/customer behavior.
  - Stratification: segment amounts by size, by token type, by counterparties (identify concentration).
  - Duplicate detection: repeated patterns / repeated fee structures indicating automated mixers or bots.
  - Frequency & velocity tests: rapid micro-transactions (dusting attacks, smurfing).
- Step-by-step: run stratification and gap detection in IDEA on the sample dataset. Interpret outputs.

Lab 2: Run stratification + gap detection; identify top 10 suspicious transaction clusters.

Session 3 — Network Analysis & Visualisation (90 min)

- Converting transaction lists into edge lists for graphing (from → to → amount → time).
- Using Gephi / Cytoscape / Neo4j for relationship mapping:
  - Node degree, in/out degree, centrality, clusters/communities.
  - Detecting mixers via hub-and-spoke patterns and circular flows.
- Demo: Build a transaction graph from the IDEA output; apply community detection; highlight likely mixer nodes.

Lab 3: Create a network graph from provided dataset; identify 3 suspicious clusters and justify why.

Session 4 — Advanced Techniques: Chain Hopping, Bridges & DeFi (60 min)

- Identifying cross-chain movement: wrapped tokens, bridge transactions, smart contract interactions.
- DeFi red flags: flash loans, liquidity pool wash trades, sudden approvals to contracts, suspicious contract deployers.
- NFTs as layering tools: wash trading, over-invoiced NFT sales, use of marketplaces to obscure provenance.

Case study (hands-on): NFT wash trade scenario — follow transaction trail and produce a short timeline.

Day 3 — Investigative Workflow, Case Studies & Reporting

Duration: 6–7 hours (capstone simulation + reporting)

Session 1 — Case Study Deep Dive #1: Darknet Marketplace (Silk Road style) (75 min)

- Scenario overview (anonymized & historic): marketplace payments into BTC, mingled via tumblers, cashed out via multiple exchanges and OTC.
- Walkthrough: timeline reconstruction, key wallet clustering, mapping cash-in points.
- Demonstration: How to request KYC/preservation from exchanges and combine on-chain evidence with off-chain data.

Exercise: Given a timeline, prepare evidence checklist and next investigative steps (law-enforcement referral, STR drafting).

Session 2 — Case Study Deep Dive #2: Sanctions & Mixer (Tornado Cash style) (60 min)

- Scenario: sanctioned entity's address receives funds and uses a mixer to obfuscate. Discuss legal/regulatory responses (sanctions designation, exchange freezes).
- How to detect mixer usage (pattern signatures), tranche analysis (entries vs exits), and linking pre-mixer and post-mixer chains.

Practical: Identify pre-mixer sources and post-mixer destination clusters from a simulated dataset.

Session 3 — Case Study #3: North-Korean APT / Lazarus-style Crypto Thefts (60 min)

- Typical pattern: theft from exchange/DeFi → laundering through mixers, bridges, chain hopping, conversion to stablecoins → withdrawal to peer-to-peer OTC.
- Indicators: large single theft, quick fragmentation, migration to privacy chains, use of decentralized exchanges.

Group task: Draft an investigative hypothesis and list operational steps to preserve evidence and disrupt laundering.

Session 4 — From Analysis to STR / Intelligence Product (75–90 min)

- What to include in a crypto-focused STR: chronology, chain evidence (txids), counterparties, value converted to fiat, typology match, recommended action.
- Attaching supporting exhibits: Sankey diagrams, adjacency tables, address labels, screenshots of explorer evidence.
- Demo: Prepare a one-page intelligence brief + STR appendix from one of the labs.

Capstone simulation (team exercise): Each team receives a full simulated case (CSV + explorer links) — detect patterns, map money trail, create a 2-page STR and present 10-minute findings to group.
