



Blockchain Forensics Framework

Version 1.1 | Effective 1 January 2026

Introduction

This framework provides Institute standards for blockchain transaction analysis, forensic investigation techniques, and evidence handling for compliance purposes. It addresses transaction tracing, red flag identification, and appropriate escalation protocols.

Authority: This framework is the authoritative reference for TCCS examination content on Domain 2 (Blockchain Forensics & Transaction Tracing). All examination marking criteria and model answers are derived from this framework.

1. Core Blockchain Forensic Techniques

Blockchain forensics relies on three core techniques:

- 1. Address Clustering:** Grouping addresses controlled by the same entity using common-input-ownership heuristics, change address patterns, and behavioural analysis.
- 2. Transaction Flow Analysis:** Tracing funds forward (where money went) and backward (where it came from) through the transaction graph.
- 3. Entity Attribution:** Linking addresses to known entities (exchanges, mixers, darknet markets) using exchange deposit/withdrawal patterns and known service addresses.

2. Red Flag Identification

Common blockchain red flags indicating potential money laundering or illicit activity:

Red Flag	Risk Level	Typical Indicator
Mixer/tumbler service usage	HIGH	ChipMixer, Wasabi, Tornado Cash exposure
Darknet market association	CRITICAL	Direct transactions to/from known DNM addresses
Sanctioned entity exposure	CRITICAL	OFAC SDN list addresses, Russian exchanges post-sanctions
High-risk jurisdiction exchanges	MEDIUM-HIGH	Exchanges in non-compliant jurisdictions, weak KYC
Peel chain structuring	MEDIUM	Sequential small withdrawals to obfuscate large sum
Privacy coin conversion (XMR, ZEC)	HIGH	BTC → XMR (Monero) swaps, untraceable conversion
Ransomware payment addresses	CRITICAL	Known ransomware wallets (Conti, Ryuk, etc.)
Rapid round-tripping	MEDIUM	Funds cycle through multiple exchanges within hours

Note: Red flags do not constitute proof of wrongdoing. They trigger enhanced investigation, not automatic rejection.

3. Red Flag Escalation Decision Logic

INSTITUTE POSITION: Escalation Thresholds

The Institute's position is that not all red flags require immediate SAR filing. Escalation should be proportionate to risk severity and context. However, CRITICAL red flags (sanctioned entities, ransomware, darknet markets) require immediate SAR filing without MLRO consultation.

Common Misapplication (Exam Risk): Candidates either (a) file SARs for every minor red flag, creating noise, or (b) wait for 'certainty' before escalating critical risks. Both approaches are incorrect.

Table 2: Escalation Decision Framework

Risk Severity	Example Red Flags	Action
CRITICAL	Sanctioned entity, ransomware, darknet market	File SAR immediately - inform MLRO concurrently - REFUSE transaction
HIGH	Mixer usage, privacy coin conversion	Consult MLRO immediately - likely SAR - consider transaction refusal
MEDIUM-HIGH	High-risk jurisdiction, peel chain, rapid round-tripping	Enhanced monitoring - consult MLRO if pattern persists - document rationale
MEDIUM	Unusual transaction timing, inconsistent with profile	Request customer explanation - document response - escalate if unsatisfactory
LOW	Single indirect exposure (3+ hops) to known service	Document in file - ongoing monitoring - no immediate escalation

Key Principle: Escalate based on red flag severity AND customer context. A single HIGH red flag with reasonable explanation may not warrant SAR. Multiple MEDIUM red flags without explanation likely do.

4. Mixer and Tumbler Analysis

INSTITUTE POSITION: Mixer Exposure Thresholds

The Institute's position is that direct mixer usage (1-hop) is a HIGH red flag requiring MLRO consultation and likely SAR. Indirect exposure (2+ hops) is contextual and should be evaluated proportionately.

Decision Logic:

Direct (1-hop): Customer's wallet → mixer → destination. HIGH risk. Consult MLRO. Likely SAR.

2-hop: Customer → intermediate address → mixer → destination. MEDIUM-HIGH risk. Request explanation. Consider SAR if unsatisfactory.

3+ hops: Customer → ... → mixer. MEDIUM or lower. Document exposure. Monitor for patterns. No automatic SAR.

Minimum Acceptable Standard: Always investigate direct mixer usage. Never automatically reject based solely on indirect exposure without context.

Common Misapplication (Exam Risk): Candidates state 'any mixer exposure requires SAR' or 'indirect exposure doesn't matter'. Both extremes are incorrect. Apply proportionate judgement.

5. Legitimate Privacy vs Suspicious Obfuscation

Not all privacy-enhancing techniques indicate illicit intent. Distinguishing legitimate privacy from suspicious obfuscation requires context.

Behaviour	Legitimate Privacy	Suspicious Obfuscation
Using new address per transaction	✓ Best practice for privacy	Only suspicious if combined with other red flags
Self-custody wallet (unhosted)	✓ Legitimate personal control	Suspicious if refuses to prove ownership or explain large movements
Multiple exchange accounts	✓ Diversification, redundancy	Suspicious if rapid round-tripping between exchanges without rationale
CoinJoin usage (e.g., Wasabi, Samourai)	⚠ Privacy tool but HIGH risk flag	Requires explanation. Often insufficient for legitimate retail use.
Lightning Network usage	✓ Legitimate Layer 2 scaling	Only suspicious if combined with other obfuscation (e.g., LN → mixer)
Privacy coins (Monero, Zcash)	⚠ Privacy-focused but HIGH risk	Conversion BTC → XMR is HIGH red flag. Requires strong justification.

Evaluation Framework: Ask: (1) Does the customer have a reasonable explanation? (2) Is the technique proportionate to their stated needs? (3) Are there multiple obfuscation layers?

6. Risk Score Interpretation and Action Thresholds

Blockchain analytics tools (Chainalysis, Elliptic, TRM Labs) provide risk scores. Institute guidance on interpretation:

Risk Score	Interpretation	Action
Severe (e.g., Chainalysis 'Severe')	Direct illicit exposure (ransomware, sanctions, DNM)	REFUSE transaction - file SAR immediately
High (e.g., Chainalysis 'High')	Significant mixer/high-risk exposure	Consult MLRO - enhanced due diligence - likely SAR
Medium	Indirect exposure or behavioral red flags	Request customer explanation - document - escalate if inadequate
Low	Minimal or distant exposure	Proceed with standard monitoring

Critical Note: Risk scores are decision support tools, not definitive verdicts. Always apply human judgement and consider customer context. Automated rejection based solely on scores is inappropriate.

7. Evidence Collection and Chain of Custody

When blockchain evidence may be used for regulatory reporting or law enforcement:

Required Documentation:

- Transaction IDs (txids) for all relevant transactions
 - Wallet addresses (originator and beneficiary)
 - Blockchain explorer screenshots (timestamped)
 - Analytics tool reports (Chainalysis PDF exports, etc.)
 - Investigation timeline (who accessed data when)
 - Analyst notes and interpretation rationale
-

INSTITUTE POSITION: Evidence Integrity

The Institute's position is that blockchain evidence is tamper-resistant but not tamper-proof. Screenshots can be edited. Maintain chain of custody by documenting who accessed evidence and when. Prefer direct blockchain queries (e.g., via node or public explorer) over third-party summaries.

Minimum Acceptable Standard: For SAR submissions, include transaction IDs that NCA can independently verify. For internal investigations, document evidence collection methodology.

TrustCrypto Institute

Blockchain Forensics Framework v1.1

Effective: 1 January 2026

(This framework is the authoritative reference for TCCS examination Domain 2)