A Practitioner's Guide to Cryptocurrency Tracing & Documentation

The Block Audit Tracing Standard (B.A.T.S.) Desk Reference

WWW.THEBLOCKAUDIT.COM

BOARD DIRECTION AND OVERSIGHT

The B.A.T.S. method intends to continuously adapt and keep pace with the everchanging world of cryptocurrency investigations through advisory board oversight. A prospective board consisting of key players in the crypto investigations space with wide reach and a common mission of delivering the highest quality and most scalable solutions in effective crypto forensics is currently being organized. This board will continues to moderate and certify training content and standards of the B.A.T.S. method to ensure the most effective solutions for practitioners. The prospective advisory board will includes the following member organizations:

- ***X State Attorney General's Office***
- ***X State University Forensic Accounting Department***
- ***X International Financial Crimes Non-Profit***
- ***X Coalition of Crypto Investigators***
- **Block Chain Intelligence Group**
- **The Block Audit LLC**

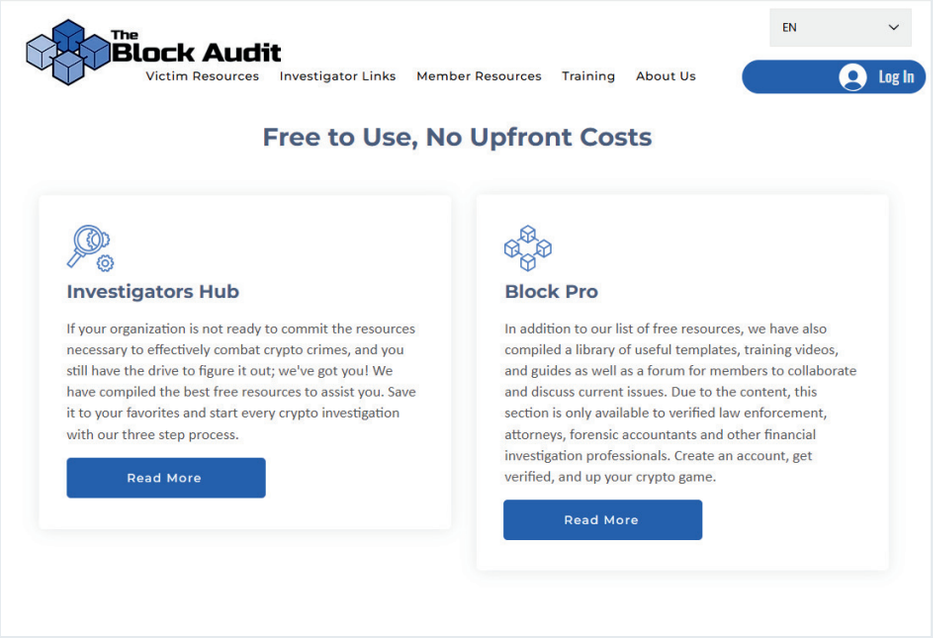
Check www.theblockaudit.com for updates on the advisory board composition as we are still finalizing agreements.

Content

Who we are...

The Block Audit LLC

The Block Audit LLC was created by active police economic crimes detectives as a way to collaborate and share lessons learned with other law enforcement and financial investigations professionals to aid in combatting the swift adoption of cryptocurrency focused tactics into traditional financial crimes cases.



Our Motivation

While attempting to stay abreast of the latest trends in financial crimes, and respond to the growing cryptocurrency related case load, we sought any relevant training. Unfortunately, there was not much available concerning how to investigate or trace cryptocurrencies. This sparked a journey that continues till this day to locate resources, decipher criminal tactics, and connect with industry experts to stay up to date with an everchanging and evolving crime trend.

We quickly learned however, that our "favorite tabs" in our internet browser was running out of space, and it was becoming increasingly difficult to organize the useful sites we were locating to assist in open-source crypto investigations. This prompted us to create www.theblockaudit.com where we could host all of these links in an organized manner, not only for our own use, but to share with other investigators who would soon be facing the same issues.

Our Vision

Equip every citizen with access to expert knowledge, experience and forensic tools in the fight against crypto facilitated crimes through partnership with law enforcement and financial investigative professionals.

954-698-2700 www.theblockaudit.com info@theblockaudit.com

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

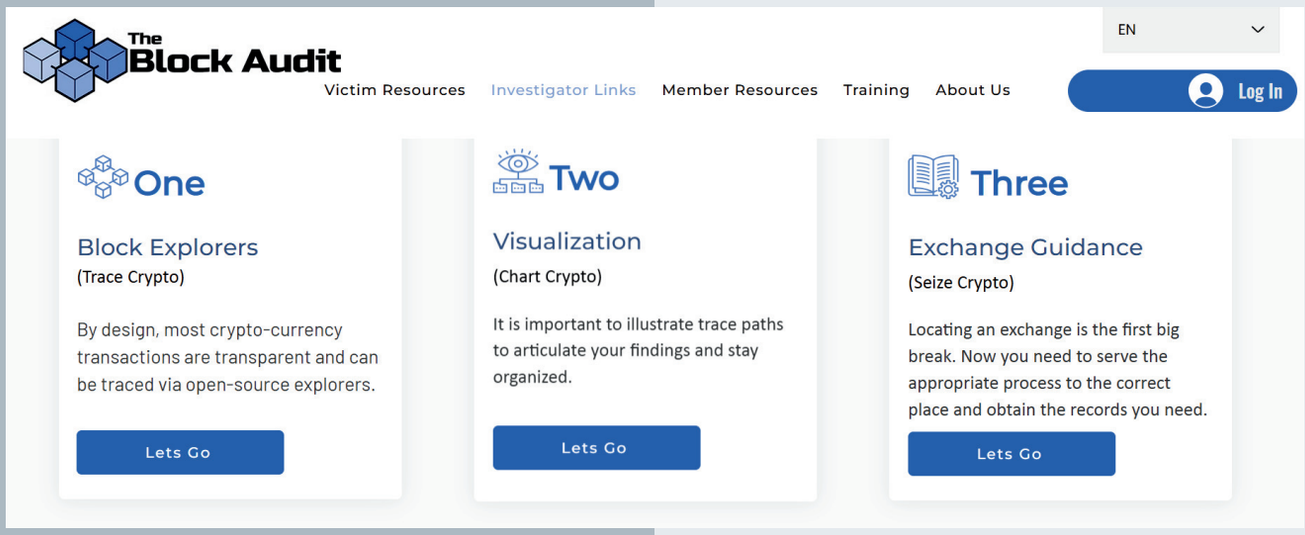
What we Offer..

Open Source Resources

Our Investigators Hub is open for anyone to use. It is a curated collection of all open source block explorers and other crypto related sites we have found to be useful in conducting real investigations. We have organized them by subject into an easy to navigate menu. Whether you are attempting to trace assets, locate crypto kiosks in your area, identify historical crypto prices, or find an efficient way to chart a graph for presentation, you will find useful links here.

Legal Service Guide

The legal landscape of crypto investigations changes by the day. Which exchanges are willing to cooperate with law enforcement and what they require in the form of legal process is a never ending struggle to keep up with. We harness our own experience and the experiences of our members to provide an updated list of where, and how to serve legal process. We also provide templates and examples to assist in your investigations.



Community of Experts

For any individual person to claim status as a "crypto expert" is a mistake when you are in a field that is constantly changing. The expertise you may have today can be completely wiped out tomorrow by a shift in this rapidly changing industry. The only way to develop true expertise is through wide collaboration in an environment where we can continuously learn from one another in this developing field. That is why we have created forums and communication channels where we as practitioners can share lessons learned and stay abreast of the latest developments in a secure area.

Training

We offer various levels of training from introductory webinars to our full 40 hour Crypto Investigators Academy. We can also develop custom courses to meet your needs. Hosting agencies will receive free seats to training.

Consulting and Blockchain Forensics

While we have taken great lengths to provide the information and tools your agency needs to be successful as a free resource, we know not everyone will have the will, resources, or manpower to dedicate to this task.

We offer a scalable turn-key solution for any entity wanting to address crypto facilitated crimes without dedicating the time, manpower, and training necessary to stand up a new unit.

For an annual subscription fee, The Block Audit will consult on policy creation, asset custody considerations, and development of investigative work flows. We will also assign dedicated Blockchain Forensic Examiners to conduct the trace of assets using our own forensic tool licenses to progress criminal investigations toward the goal of case closures, victim asset recovery and/or asset forfeiture.

Glossary of Terms

Adjusted Root Total (ART): The root minus any documented write-offs. This becomes the accounting baseline that all threads must sum to at each hop level for mathematical validation.

Back Tracing: The investigative technique of working backward from known criminal infrastructure or terminal wallets to identify additional victims or funding sources. When performed during Level 3 or 4 investigations, back tracing functions as Level 1 discovery - prioritizing speed and lead generation over detailed documentation.

Block Audit Tracing Standard (B.A.T.S.): A standardized framework for cryptocurrency investigation that maintains the golden thread of traceability required for successful asset forfeiture cases through systematic color classification, hierarchical notation, and accounting validation.

Cluster Analysis: Examines relationships and patterns across multiple addresses without focusing on specific transaction flows, identifying relationships through behavioral patterns revealing common ownership.

Commingling: When traced criminal proceeds mix with existing wallet balances or other fund sources, requiring careful application of PIFO principles to maintain the golden thread. Courts have established that commingling does not cleanse tainted funds.[6]

Convergence: When multiple trace paths arrive at the same wallet and subsequently move out together as a single transaction. Requires application of the Sequential Hop Rule.

Exchange Deposit Addresses: Wallets where the on-chain trail terminates and legal process becomes necessary to continue tracing. Classified as PURPLE wallets in B.A.T.S.

Golden Thread: The unbroken connection between a victim's original funds and any assets ultimately seized by law enforcement, essential for proving direct traceability in asset forfeiture cases. This principle aligns with judicial standards that examine direct connections between assets and criminal activity.[4]

High-Risk Customer: A customer or wallet identified through risk assessment procedures as presenting elevated money laundering or terrorist financing risk based on factors such as transaction patterns, geographic exposure, or business type.

Hop Count: The measurement of distance from the victim-facing wallet rather than chronological discovery order. Each blockchain transaction increments the hop count by one.

Hub Wallets: Wallets where multiple victim traces converge, proving common criminal control. Classified as YELLOW wallets and crucial for linking separate criminal operations.
LIBR Method (Lowest Intermediate Balance Rule): An alternative to PIFO that tracks funds based on the lowest balance point between deposits and withdrawals.[1][2]

LIBR Method (Lowest Intermediate Balance Rule): Traditional asset tracing principle applicable to cryptocurrency investigations that tracks the lowest balance point in an account to determine maximum traceable amounts. Has the effect of holding tracible assets to fewer hops.

Matching Transactions Principle (MTP): An exception to strict PIFO methodology when outgoing transactions precisely match incoming thread totals in amount and occur in close temporal proximity.[3]

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

Glossary of Terms

Off-Ramping: The process by which criminals convert cryptocurrency to fiat currency or other assets, typically through exchanges.

On-Ramping: The process by which stolen funds initially enter the criminal cryptocurrency infrastructure**.**

PIFO Method: (Proceeds In First Out) - the principle that when traced funds enter a wallet, the very next outbound transaction contains those funds, applied chronologically. This method is often mischaracterized as first-in-first-out, but PIFO works fundamentally different as the practice of following “dirty” funds does not reset upon each subsequent deposit to the wallet, and PIFO is grounded in its own specific case law.; not inventory accounting methods.[1][2]

Red Wallet Index: The formal inventory of all victim-facing wallets (RED wallets) identified in an investigation, with each assigned a permanent identifier (R1, R2, R3, etc.).

Root: The original amount of a victim's transaction that forms the baseline for all subsequent tracing.

Root Validation: The mathematical verification process ensuring that all thread totals at any given hop level sum to the adjusted root total, providing proof of investigation completeness and preventing scope creep.

Sequential Hop Rule: The rule for handling convergence by applying the highest hop count among all converging paths, plus one for the outbound transaction.

Thread: The specific amount being traced through a particular transaction path at any given hop level.
Thread Exposure: The percentage of a wallet's total balance comprised of traced criminal proceeds.

Travel Rule: Regulatory requirement mandating that VASPs collect and transmit specific originator and beneficiary information for cryptocurrency transfers exceeding designated thresholds.[5]

Universal Wallet Index (UWI): A comprehensive index of all wallets involved in the money laundering process.

V-T-H Notation: The standardized identification system where V represents victim number, T represents transaction number, and H represents hop count from the victim-facing wallet.

V-T Notation: The standardized identification system used in B.A.T.S. 3 where V represents victim number, T represents transaction number.

Victim Facing Wallets: The first wallets to receive stolen funds where criminal acts are initiated. Classified as RED wallets and serving as the starting point for all hop counting.

Write-off: Documented abandonment of trace paths for practical reasons including dust amounts, dilution, obfuscation, or operational constraints.

Legal Standards and Jurisdictional Considerations

Application of Legal Precedents in B.A.T.S.

The Block Audit Tracing Standard (B.A.T.S.) references various court decisions and legal precedents throughout this guide to illustrate established principles in asset tracing and forfeiture. These citations represent examples of judicial reasoning that the developers of B.A.T.S. believe demonstrate best practices for conducting thorough and legally sound cryptocurrency investigations.

Important Jurisdictional Notice: Legal precedents and their application can vary significantly by jurisdiction. The court cases referenced in this guide—including decisions from the Second Circuit, Seventh Circuit, Southern District of New York, and other federal courts—are provided as illustrative examples only. Different jurisdictions may have established different standards, requirements, or interpretations regarding:

- Asset tracing methodologies (PIFO vs. LIBR)
- Commingling and tainted funds
- Direct traceability requirements
- Evidentiary standards for forfeiture

Core Principles Remain Constant

While specific legal requirements may differ, the core principles of B.A.T.S. remain universally applicable:
Mathematical Precision: Maintaining accurate accounting throughout investigations
Documentation Standards: Creating clear, reproducible audit trails
Golden Thread Methodology: Preserving traceable connections between crimes and assets
Systematic Classification: Using consistent wallet categorization
Validation Processes: Ensuring investigative completeness through root validation
These fundamental principles strengthen any investigation regardless of jurisdictional requirements.

Practitioner Guidance

This reference guide is not intended to supersede or replace the legal standards established in your particular jurisdiction. Investigators and compliance professionals using B.A.T.S. methodology should:
Consult with Legal Counsel: Work closely with your organization's legal advisors to understand applicable precedents in your jurisdiction
Coordinate with Prosecutors: Engage early and often with prosecutors handling your cases to ensure investigative methods meet local evidentiary requirements
Adapt as Necessary: While maintaining B.A.T.S. core principles, adapt specific applications to meet jurisdictional requirements
Document Deviations: If local requirements necessitate modifications to B.A.T.S. methodology, document these adaptations and their legal basis
Stay Current: Legal standards for cryptocurrency investigations continue to evolve rapidly; maintain awareness of new precedents in your jurisdiction and maintain compliance with all updates to the B.A.T.S. method.

Legal References

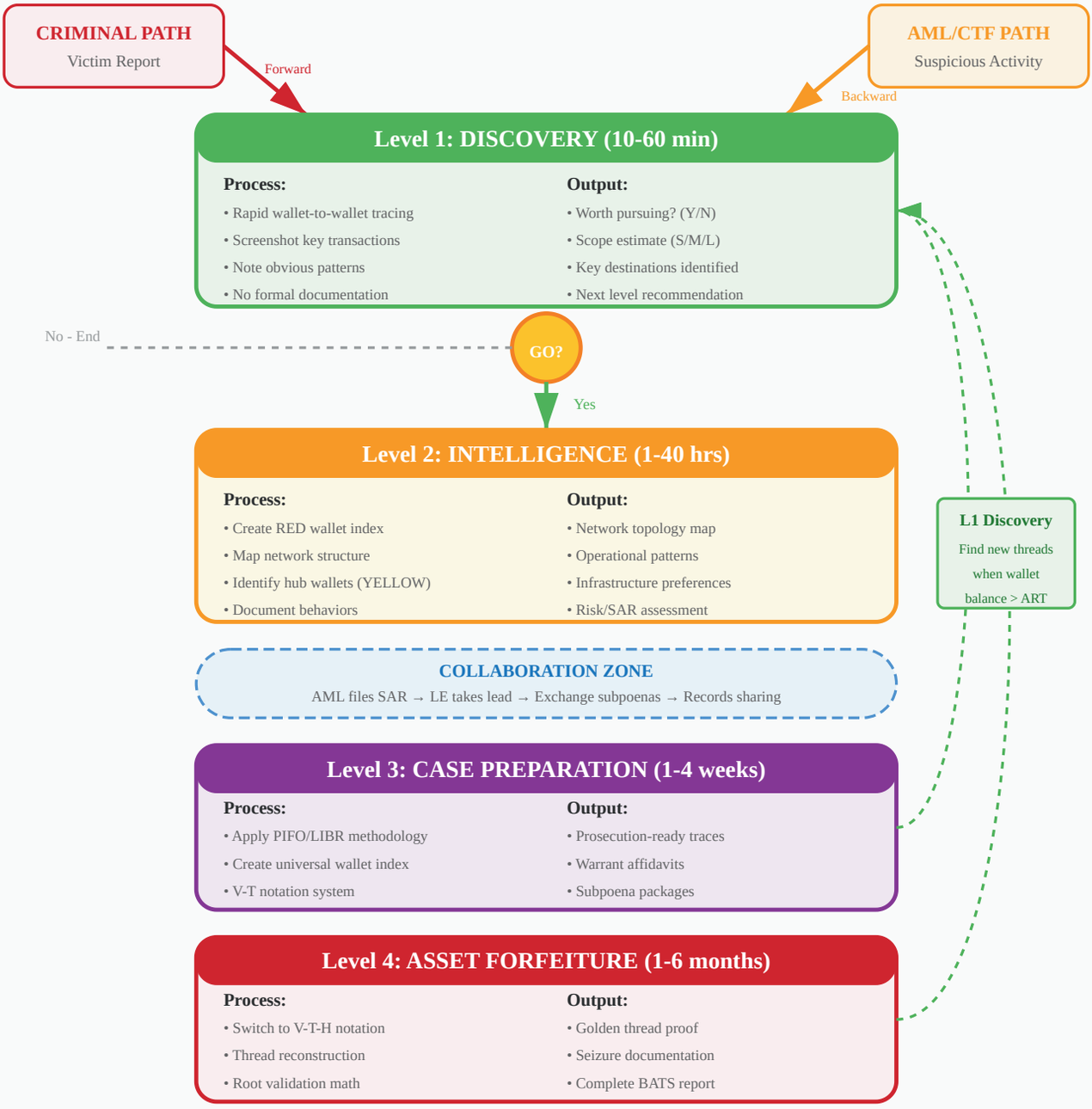
[1] United States v. Banco Cafetero Panama, 797 F.2d 1154 (2d Cir. 1986); United States v. Banco Cafetero Int'l, 608 F. Supp. 1394 (S.D.N.Y. 1985).
[2] United States v. $448,342.85, 969 F.2d 474 (7th Cir. 1992).
[3] United States v. $557,933.89, 287 F.3 nd 66, 77-78 (2d Cir. 2002); In re Marriage of Wren, 338 Ill. App. 3d 1067, 1074 (2003).
[4] United States v. Funds in the Amount of $239,400, 795 F.3d 639, 642-43 (7th Cir. 2015); United States v. Thirteen Million Dollars, 733 F. Supp. 2d 834, 837 (W.D. Tex. 2010).
[5] FATF Recommendation 16 (2012, updated 2023); 31 CFR § 1010.410(f).
[6] United States v. All Funds on Deposit at Wells Fargo, 643 F. Supp. 2d 577, 582-83 (S.D.N.Y. 2009).

The legal citations provided represent examples of relevant precedents and are not exhaustive or authoritative. Practitioners should research current applicable law in their jurisdiction.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

B.A.T.S. Framework: Investigation Mechanics

How Criminal and AML Investigations Converge Through Standardized Methodology



Core Mechanics

- **Wallet Classification:** RED (victim-facing) → YELLOW (hubs) → PURPLE (exchanges) → Terminal points
- **Notation Evolution:** Informal (L1) → Wallet-centric V-T (L3) → Transaction-centric V-T-H (L4)
- **Documentation:** Screenshots → Behavioral analysis → Legal narratives → Mathematical proof
- **Methodology:** Pattern recognition → Network mapping → PIFO/LIBR → Root validation

Wallet Classification System

Before diving into the specific levels, it's essential to understand the wallet classification system used throughout the B.A.T.S method. This color-coding system transforms complex wallet analysis into immediately recognizable categories:

RED wallets: Victim facing wallets – the first destination for stolen funds where the criminal act is initiated. These wallets provide undeniable evidence of criminal activity and serve as the starting point for all hop counting.

PINK wallets: Dividend and deception operations where fake returns are sent to victims in investment scams. PINK classification provides undeniable proof of criminal intent and serve to implicate all black wallets between them and the red wallets as part of the criminal network.

YELLOW wallets: Hub wallets where multiple victim traces converge. This convergence proves common criminal control and also serve to tie in any black wallets occurring between them and the initial red wallets as participating in the criminal network.

ORANGE wallets: Bitcoin change addresses essential for UTXO tracing.

BROWN wallets: Handle asset conversion where cryptocurrency types change via bridges, decentralized exchanges, or DApps. These are on-chain services where the color-coded indicator can be used to note changes in assets without need to plot complex smart contract call asset flows.

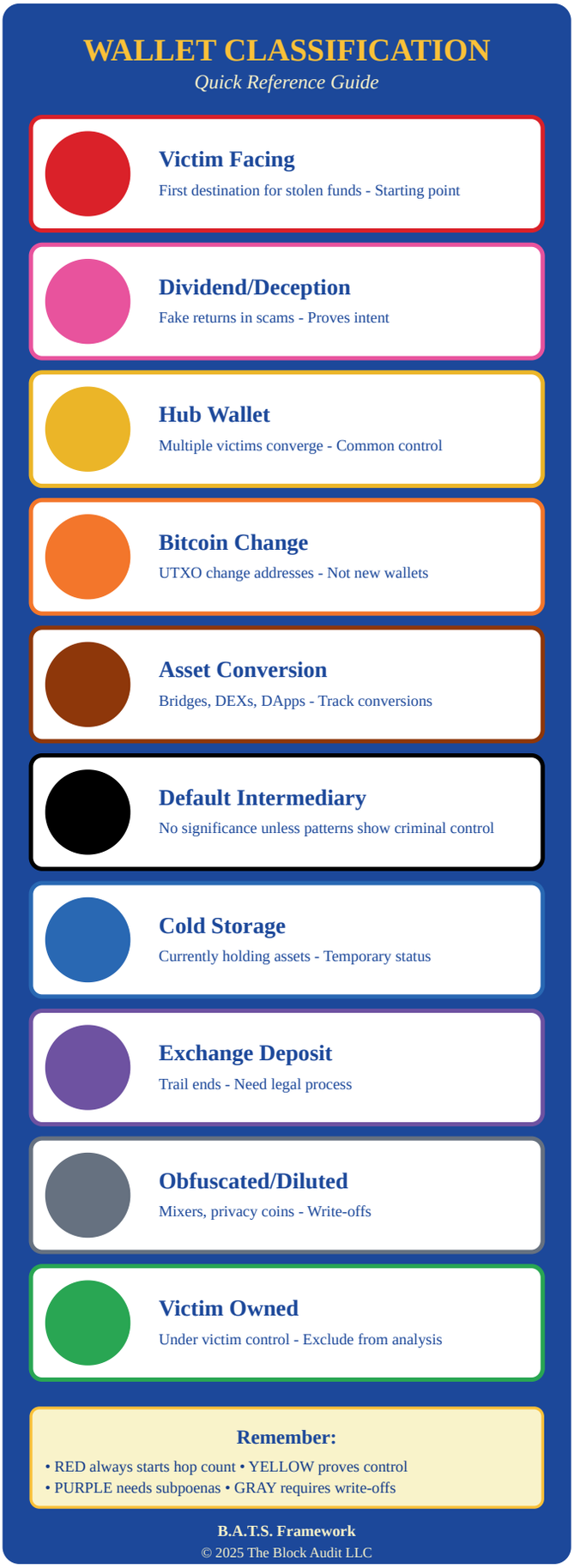
BLUE wallets: Cold storage – wallets currently holding traced assets. This is a temporary classification used to pause tracing at a specific point to await further movement or note aggregation of funds in a criminal network.

PURPLE wallets: Exchange deposit addresses where the on-chain trail terminates. These points indicate the need for legal process to obtain records to pursue the trace, identify suspects, or seize assets.

BLACK wallets: Default classification for intermediary wallets with no direct victim exposure.

GRAY wallets: Obfuscated or diluted traces where the path has become effectively untraceable. This classification is used to visually note the location where portions of the traced assets were abandoned.

GREEN wallets: Victim-owned addresses that remain under victim custody or control.



 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

A Practitioner's Guide to Crypto Asset Tracing: B.A.T.S Framework Desk Reference

Introduction: Defining The Investigative Approach

Dual Purpose Framework
The B.A.T.S. framework serves both criminal investigators and AML/CTF professionals, providing a standardized methodology that scales from rapid suspicious activity assessment to meticulous asset forfeiture documentation. This universality emerges from a fundamental principle: both groups are measuring "distance from bad" - whether that starting point is a victim's stolen funds, a known terrorist funding source, or a sanctioned entity's wallet.

Cryptocurrency investigations serve different purposes that require varying levels of precision and documentation. Sometimes you need to quickly assess if a case is worth pursuing. Other times you're building evidence that must survive courtroom scrutiny. At the highest level, you need mathematical precision to support the seizure or forfeiture of cryptocurrency assets.

The key is matching your approach to your goals. Using detailed methodology when you just need leads wastes time. Using shortcuts when you need court-ready evidence can destroy your case. Using Level 3 evidence standards when you need to seize assets can result in successful criminal prosecutions but failed asset recovery - meaning victims don't get compensated and criminals keep their proceeds.

This guide presents a comprehensive framework that scales from quick discovery to rigorous mathematical analysis. Understanding when to use each approach makes your investigations more efficient and successful, while at the highest level, the Block Audit Tracing Standard (B.A.T.S.) provides the mathematical precision required for asset forfeiture cases.

Choosing the Right Approach: Decision Framework

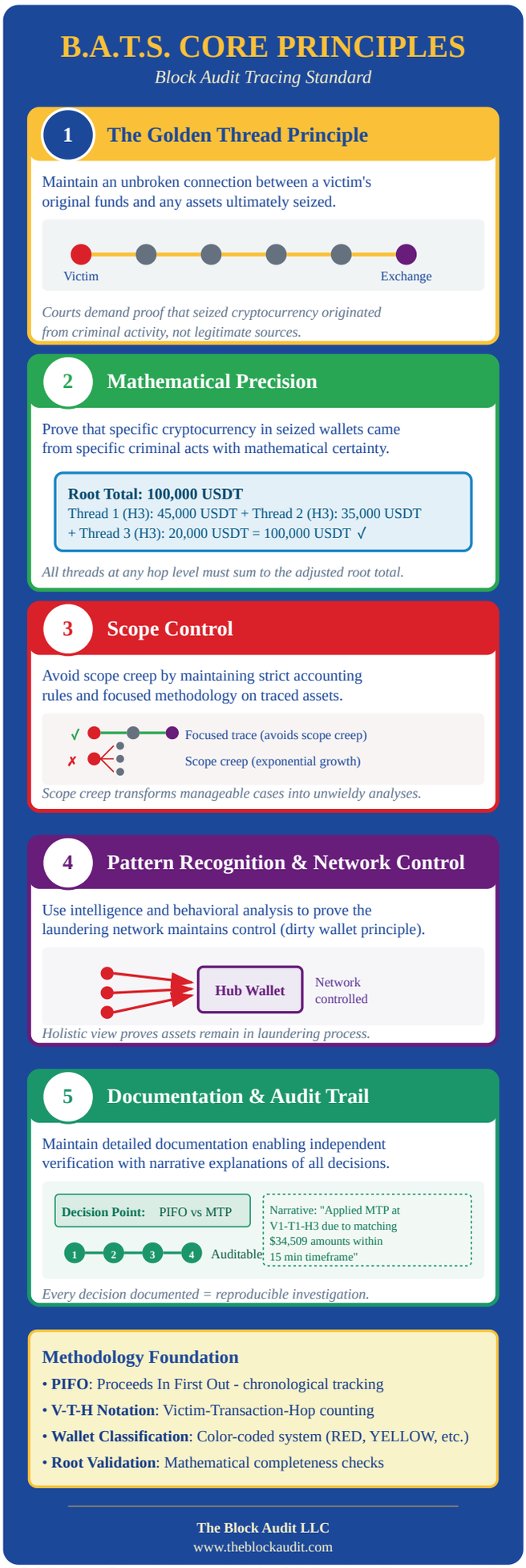
Start with Your Goals
The most important factor in choosing your approach is understanding what you're trying to accomplish: Triage, intelligence gathering, prosecution case preparation, or asset forfeiture.

Consider Your Resources
Different approaches require different time investments:
Limited time or multiple cases? Level 1 gives you the most information quickly. *Adequate resources for thorough analysis?* Higher levels provide more comprehensive results.
Specialized cryptocurrency expertise available? Level 3 and 4 approaches become more feasible.

Think About Legal Requirements
Your legal objectives determine your minimum documentation standards: Asset seizure planned? Level 4 mathematical precision is required. Search warrants needed? Level 3 case preparation is the minimum. Intelligence product sufficient? Level 1 or 2 analysis may be adequate.

Plan for Case Evolution
Many cases start at one level and evolve to require higher levels of analysis. A case might begin as Level 1 discovery to assess scope, develop into Level 2 intelligence development as patterns emerge, progress to Level 3 case preparation when suspects are identified, and finally require Level 4 asset forfeiture analysis when seizure opportunities arise.

Design your documentation to support this evolution. Even during initial discovery, maintain standards that will allow you to escalate your analysis if circumstances change. The wallet numbering system must remain stable and permanent once established in Level 2 - wallet IDs assigned never change when transitioning between levels.



The Block Audit Tracing Standard (B.A.T.S.)

Core Principles

The Block Audit Tracing Standard (B.A.T.S.) represents a revolutionary approach to cryptocurrency investigation that addresses the most critical challenge facing virtual asset forensics: maintaining the golden thread of traceability required for successful asset forfeiture cases.

The Golden Thread Principle*:* B.A.T.S. maintains that investigators must be able to prove a direct, unbroken connection between a victim's original funds and any assets ultimately seized by law enforcement. This principle addresses the fundamental legal requirement in asset forfeiture cases, where courts demand evidence that specific seized cryptocurrency originated from criminal activity rather than legitimate sources.

Mathematical Precision Requirements: Asset forfeiture requires mathematical certainty. You must be able to prove that specific dollars in seized wallets came from specific criminal acts. This isn't just following money from point A to point B - it's maintaining an unbroken mathematical connection through complex money laundering schemes.

Scope Control: The golden thread concept becomes particularly crucial when dealing with commingling, where criminal proceeds mix with existing wallet balances or other fund sources. Without rigorous methodology for tracking specific portions of commingled funds, investigations risk exponential scope creep. B.A.T.S. prevents this expansion through strict accounting rules that maintain focus on the original root total while providing mathematical validation of investigative completeness.

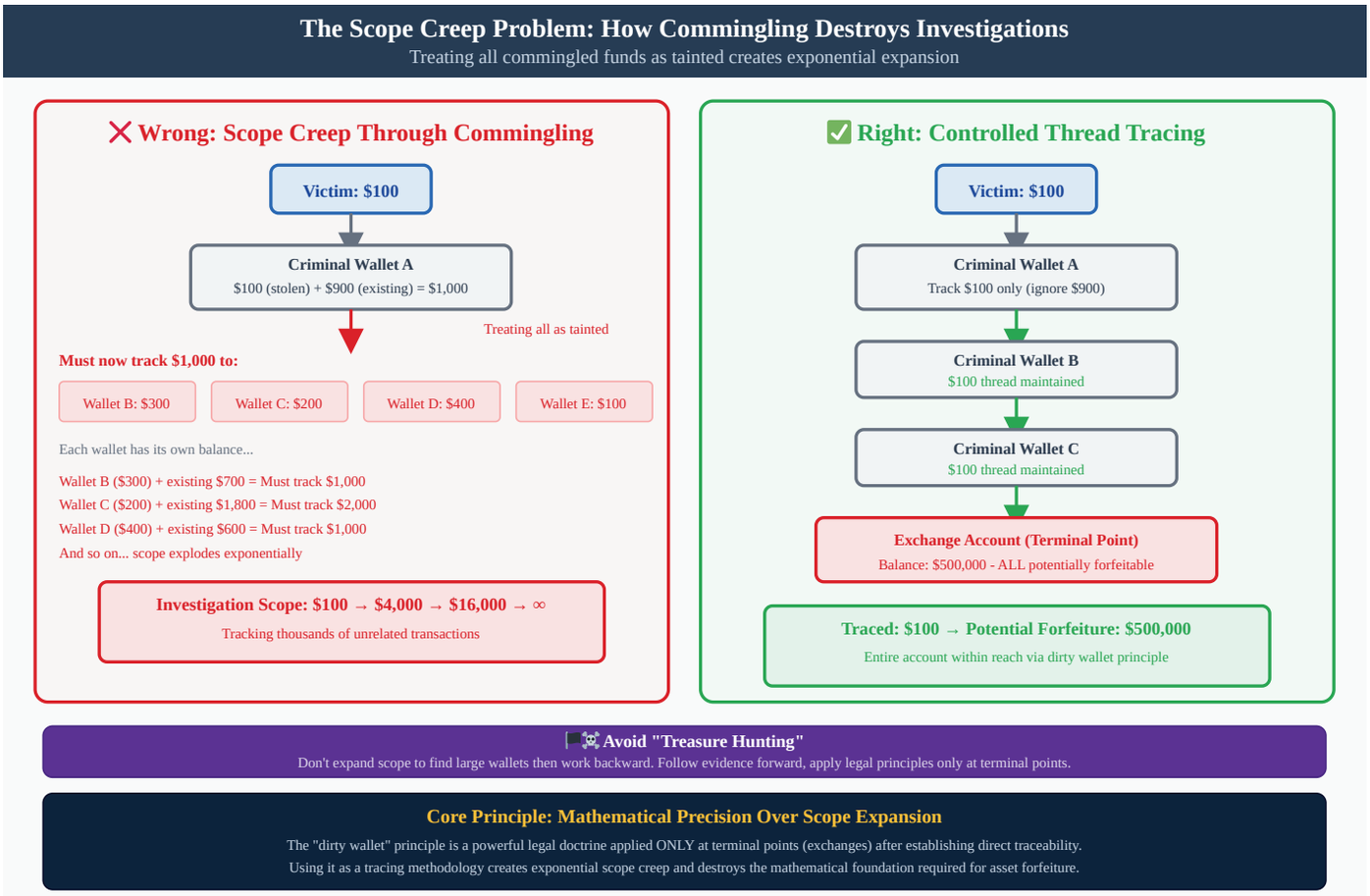
The Dirty Wallet Principle: When cryptocurrency wallets demonstrate systematic patterns of receiving funds from multiple criminal sources, this behavioral evidence may support expanded legal theories beyond traced amounts. The 'dirty wallet' principle recognizes that wallets showing these patterns of use may become instrumentalities to the crime in and of themselves, which may allow different legal treatment than wallets with incidental exposure. To prevent uncontrolled scope creep this principle should be reserved for terminal wallets potentially exposing entire wallet balances to seizure/forfeiture. B.A.T.S. documentation captures these behavioral patterns to support whatever legal theories prosecutors may pursue.

PIFO Method and Transaction Flow Principles

The cornerstone of B.A.T.S.'s transaction tracing methodology is the *PIFO method - Proceeds In First Out*. This principle maintains that when traced funds enter a wallet, the very next outbound transaction contains those funds. PIFO operates on strict chronological order, where the first proceeds to arrive are literally the first proceeds to leave.

PIFO provides the legal foundation for maintaining the golden thread through commingling scenarios. When a wallet contains both traced criminal proceeds and existing legitimate funds, PIFO enables investigators to follow the specific criminal proceeds without expanding scope to include the entire wallet balance.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.



Matching Transactions Principle (MTP)

B.A.T.S. recognizes that strict PIFO application may occasionally miss obvious criminal intent when specific amounts create clear patterns. The *Matching Transactions Principle* provides a rare exception to PIFO methodology when outgoing transactions precisely match incoming thread totals in amount and occur in close temporal proximity.

EX). If a thread total of $34,509 enters a wallet, and while strict PIFO would follow a subsequent $100,000 outbound transaction, investigators may opt to follow a later $34,509 outbound transaction if the amount specificity suggests intentional movement of those exact assets. This deviation requires documentation and narrative justification. This process does not apply the same way in UTXO blockchains where specific UTXOs in a wallet will always have matching outbound UTXOs to a transaction. (The principle still applies but care must begiven to trace value, not UTXOs. But we will cover more on this later.)

The Commingling Challenge and Scope Management

When criminal proceeds mix with legitimate funds, investigators face complex questions about which portions of subsequent transactions represent traceable criminal activity. Legal principles recognize that wallets used for money laundering may expose their entire contents to forfeiture. However, automatic application of this principle creates dangerous scope creep.

Consider tracing $100 in criminal proceeds entering a wallet containing $100 in legitimate funds. Treating the entire $200 as "dirty" and following $1 payments to 200 different wallets suddenly expands the investigation to $20,000 across 200 addresses. This exponential growth pattern can transform manageable investigations into unwieldy analyses involving thousands of addresses far removed from original criminal activity.

Effective scope management requires applying commingling principles with focused direction and clear legal justification. Consider the wallet's primary purpose, the proportion of criminal versus legitimate funds, evidence of intentional laundering versus incidental mixing, and practical constraints.

Documentation becomes crucial when applying commingling theories. Distinguish between amounts directly traceable to criminal activity and amounts included through commingling arguments. This transparency enables legal review and prevents overreach accusations. The commingling (dirty wallet) principle should be applied at terminal points after mathematical tracing establishes criminal connections, not as a methodology to expand scope during analysis.

The Treasure-Hunting Problem: A critical ethical issue emerges when investigators use broad scope expansion to locate large cryptocurrency holdings rather than following specific evidence. This approach inverts proper methodology—identifying "treasure" first, then constructing arguments to connect it to the case. Such approaches undermine the mathematical precision that gives cryptocurrency investigations legal credibility and represent overreach that courts may reject.

Proper investigation requires applying consistent methodology and accepting whatever destinations the evidence leads to. Mathematical rigor makes cryptocurrency tracing legally powerful, but this depends on following evidence rather than desired outcomes.

Professional Standards and Ethical Considerations

The field of cryptocurrency investigation operates within a rapidly evolving regulatory landscape where legal precedents continue to develop and established frameworks often lag behind technological capabilities. This dynamic environment creates both unprecedented investigative opportunities and significant professional responsibilities.

Fundamental Professional Obligations
Cryptocurrency investigators bear multiple competing but equally essential responsibilities that must be balanced throughout every investigation. The protection of the financial system represents a foundational obligation that recognizes cryptocurrency's role in the broader economy. Investigators serve as guardians against criminal exploitation while helping demonstrate that these technologies can operate safely within established legal frameworks.

Simultaneously, investigators carry responsibility to hold criminal actors accountable through thorough, accurate analysis that supports successful prosecutions. The technical complexity of cryptocurrency investigations magnifies the importance of this responsibility, as analytical errors or methodological shortcomings can undermine entire prosecutions.

The support of victim asset recovery represents another crucial obligation that acknowledges the human cost of cryptocurrency crimes. However, these obligations must be balanced against equally important responsibilities to avoid investigative overreach and prevent abuse of asset forfeiture laws.

The Precedent Development Challenge
The current regulatory environment can be characterized as a period of rapid development where many fundamental questions remain unresolved. This regulatory uncertainty presents both opportunities and dangers for cryptocurrency investigators. The absence of restrictive precedents may enable creative analytical approaches, but this apparent freedom carries significant risks.

Overly aggressive or questionable investigative techniques may ultimately prompt restrictive regulatory responses that limit future investigative capabilities. Court decisions establishing precedents for cryptocurrency investigations often result from cases where investigative techniques face legal challenges. Investigators who employ questionable methods risk creating unfavorable case law that restricts future investigations.

Professional Standards and Sustainable Practices
The development of sustainable cryptocurrency investigation practices requires conscious attention to professional standards that promote effective law enforcement while preserving individual rights and maintaining public trust.

Proportionality requires matching investigative intensity to the severity of suspected criminal activity and the strength of available evidence. Transparency in methodology builds credibility and supports legal review of investigative findings. Scope discipline requires investigators to resist expanding investigations simply because technological tools make broader analysis possible.

The maintenance of professional standards equivalent to those applied in traditional financial investigations ensures that technological complexity does not justify relaxed ethical obligations.

Building Long-Term Credibility
The ultimate goal of professional cryptocurrency investigation is developing practices that remain effective, legally defensible, and sustainable over the long term. Continuous professional development ensures investigators remain informed about evolving standards. Active participation in professional organizations enables contribution to responsible standards development.

The cryptocurrency investigation field will be fundamentally shaped by the choices that current practitioners (you and I) make today regarding professional standards and ethical constraints. By exercising appropriate restraint, maintaining high professional standards, and considering long-term implications of investigative techniques, practitioners can help ensure that powerful legal tools for asset recovery remain available for legitimate law enforcement purposes.

UTXO Tracing Considerations for Bitcoin Investigations

Bitcoin's UTXO (Unspent Transaction Output) model requires specific consideration in asset tracing methodology that differs from account-based cryptocurrencies like Ethereum. While UTXOs are technically distinguishable, Bitcoin remains fungible —each satoshi is as valuable and interchangeable as any other, similar to how serialized dollar bills remain fungible currency so that the specific serial number or physical bill is not as important in tracing as the value it represents.

The UTXO Direct Tracing Problem: Current industry practice often advocates tracing specific UTXOs through transactions, waiting for the exact UTXO from a victim's payment to move before continuing the trace. This approach violates fungibility principles and injects randomization into investigations. Wallet software autonomously selects which UTXOs to spend based on technical optimization (minimizing fees, avoiding change), not criminal intent. Following specific UTXOs disconnects the trace from timing and amount factors that would otherwise reveal suspect motives and behavioral patterns.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

P.I.F.O. METHOD

Proceeds In First Out

Core Principle

When traced criminal proceeds enter a wallet, the **very next outbound transaction** contains those funds.

PIFO Scenarios

Scenario 1: Basic PIFO

$5,000	Existing legitimate funds	*(Jan 1, 09:00)*
$3,000	Criminal proceeds arrive	*(Jan 1, 14:30)*

Balance: $8,000 | Next out = $3,000 criminal

Scenario 2: Partial Outflow

$5,000	Existing legitimate funds	*(Jan 1, 09:00)*
$3,000	Criminal proceeds arrive	*(Jan 1, 14:30)*
$1,500	First out (partial criminal)	*(Jan 1, 15:00)*

Balance: $6,500 | Remaining criminal: $1,500

√ Next $1,500 out = remaining criminal proceeds

Scenario 3: New Funds After Criminal

$5,000	Existing legitimate funds	*(Jan 1, 09:00)*
$3,000	Criminal proceeds arrive	*(Jan 1, 14:30)*
$2,000	New legitimate funds arrive	*(Jan 1, 16:00)*

Balance: $10,000 | Next out = $3,000 criminal

√ PIFO: Criminal proceeds still go out first

PIFO Application Steps

1. Identify when criminal proceeds enter wallet
2. Find the chronologically next outbound transaction
3. Follow that transaction (regardless of amount)
4. Continue PIFO at each subsequent wallet

Legal Foundation

PIFO maintains the **golden thread** of traceability through commingling scenarios. This methodology aligns with established federal precedent recognizing PIFO as a valid method for tracking fungible assets through mixed accounts.

See: U.S. v. Banco Cafetero Panama, 797 F.2d 1154 (2d Cir. 1986)

B.A.T.S. Framework
Block Audit Tracing Standard

Cluster Tracing Limitations: While clustering wallet addresses under common ownership is crucial for network analysis and intelligence gathering, using clusters in asset tracing immediately substitutes traceable assets for non-traceable ones. This breaks the golden thread required for legal recovery. Consider three separate bank accounts (A, B, C) under one login: if account A contains $100,000 pre-existing funds and stolen money gets deposited into account C, moving the original funds from account A does not implicate those funds as traceable to the crime.

B.A.T.S. Position: The PIFO (Proceeds In First Out) method and traditional asset tracing principles remain applicable to UTXO transactions when properly applied. Rather than following specific UTXOs or cluster-wide activity, investigators should focus on wallet-level behavior and transaction timing that preserves the connection between criminal proceeds and subsequent movements. This approach maintains both technical accuracy and legal defensibility while avoiding the randomization effects of UTXO-specific or cluster-based tracing.

This methodology represents a contested position within the cryptocurrency investigation community, as it challenges prevailing industry practices encouraged by major blockchain intelligence companies. However, as cryptocurrency investigations mature and face increased legal scrutiny, maintaining alignment with established financial investigation precedents becomes essential for preserving the legal basis for asset recovery.

LIBR versus PIFO: Choosing Your Methodology

LIBR and PIFO represent fundamentally opposing philosophies about how criminals handle stolen funds, and investigators must understand this philosophical divide to make informed choices:

LIBR (Lowest Intermediate Balance Rule) operates on the principle that criminals have no authority to pass title on stolen property. This method seeks to preserve the tainted nature of funds as long as possible, tracking based on the lowest balance point between deposits and withdrawals. LIBR essentially argues that stolen funds "stick" to an account until the balance forces them out.

PIFO (Proceeds In First Out) assumes criminals inject ill-gotten gains into the money laundering process as quickly as possible, attempting to distance their proceeds from the crime and obfuscate the trail.

These methods are directly at odds with one another, yet B.A.T.S. supports both approaches, recognizing that different investigations may benefit from different methodologies. The critical requirement is consistency: once an investigator chooses a method at the start of an investigation, they must apply it throughout. B.A.T.S. does not permit arbitrary switching between methods to engineer favorable outcomes.

Practical Considerations for Method Selection:

- Use LIBR when: You need to limit hop counts and conserve value in wallets that may be within reach of successful seizure through stablecoin burn and reissue tactics, or when dealing with wallets showing patterns of accumulation before movement.

- Use PIFO when: You're following assets likely to flow through to VASPs where seizure requires cooperation with centralized entities, or when criminal patterns suggest rapid fund movement.

The choice often depends on your seizure strategy: LIBR may keep funds "closer" to the crime and within reach of novel seizure methods, while PIFO may better reflect actual criminal behavior in high-velocity money laundering operations.

Universal Standards Across All Levels

Regardless of which method you choose or at which investigation level you begin, certain principles apply to all cryptocurrency investigations:

Make It Reproducible: Another investigator should be able to follow your work and reach the same conclusions. Document your sources, your reasoning, and your analytical choices.

Be Transparent About Limitations: If you can't trace certain funds or had to make assumptions, say so clearly. Honesty about limitations builds credibility.

Maintain Consistent Standards: If you decide to use a particular tracing method for some parts of your investigation and deviate for others, be clear about where you're applying which method and articulate your reasoning for the change.

Keep the End Goal in Mind: Even during early-stage analysis, consider what type of evidence you might eventually need and document accordingly.

Technical Consistency

Verify Wallet Addresses: Double-check addresses to prevent transcription errors that can invalidate your analysis.

Use Standard Time Zones: Document all timestamps in UTC to avoid confusion.

Save Transaction Hashes: Preserve the unique identifiers that let others verify your findings.

Take Consistent Screenshots: Develop standard procedures for visual evidence whether that be opensource explorer tools or graph exports from your preferred forensic tool.

Analytical Frameworks: Transaction Analysis versus Cluster Analysis

Transaction analysis maintains mathematical traceability between specific transactions and amounts, treating each transaction as discrete movement of identifiable funds. This approach enables investigators to demonstrate that particular cryptocurrency holdings represent specific criminal proceeds, making it essential for asset forfeiture cases.

Cluster analysis examines relationships and patterns across multiple addresses without focusing on specific transaction flows, identifying relationships through behavioral patterns revealing common ownership. This methodology supports intelligence development and network mapping by revealing criminal organization structure.

Specialized Investigation Applications

Travel Rule Compliance, AML Investigation, and SAR Production

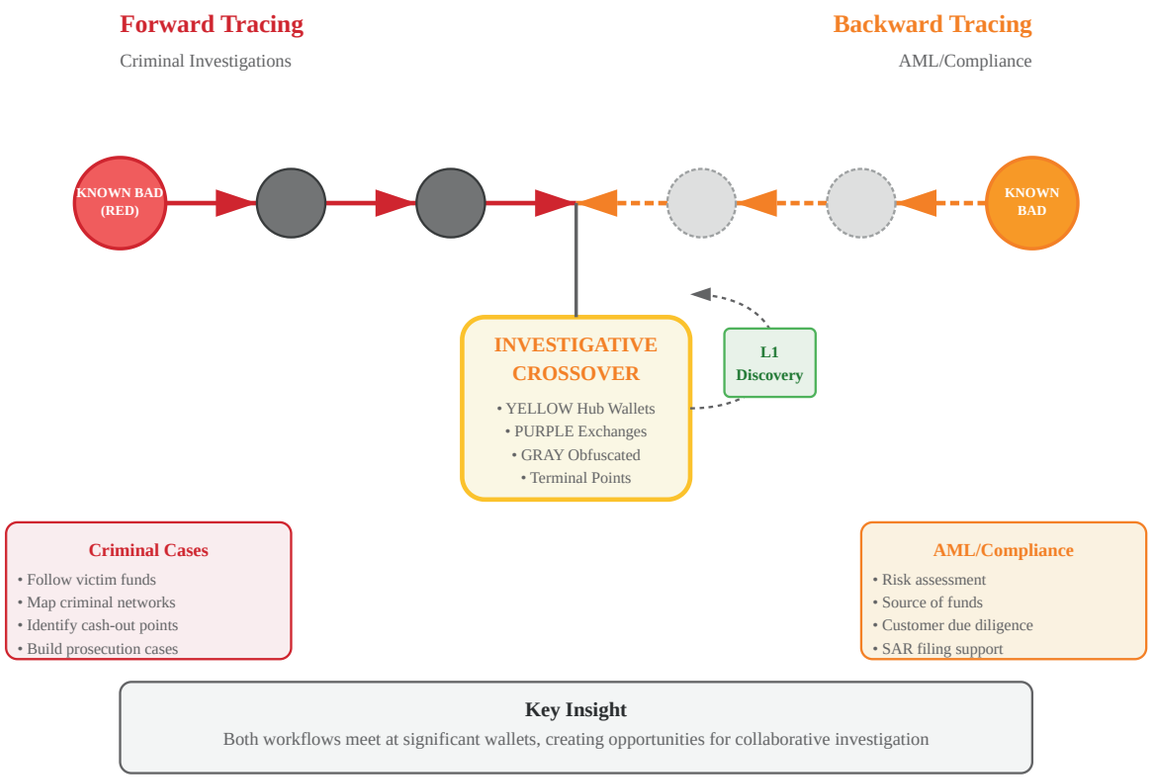
SAR Production Requirements vary significantly based on complexity. Simple SAR filings may require only Level 1 discovery techniques to document basic transaction patterns. Complex suspicious activity involving sophisticated money laundering typically requires Level 2 intelligence development. When SAR filings relate to ongoing law enforcement investigations, coordination may require Level 3 case preparation standards.

Travel Rule Documentation Requirements mandate that Virtual Asset Service Providers collect and transmit specific information about cryptocurrency transfers exceeding regulatory thresholds. Investigations typically begin with Level 1 discovery techniques but may require Level 2 intelligence development for complex compliance scenarios or Level 3 standards for regulatory proceedings.

AML Risk Assessment Investigations vary in scope based on institutional risk tolerance and regulatory expectations. Basic AML screening might employ Level 1 discovery techniques, while comprehensive analysis for high-risk customers may require Level 2 intelligence development. AML violations requiring enforcement action typically escalate to Level 3 case preparation standards.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

Forward vs Backward Tracing: Two Paths, One Goal



Directional Analysis: Forward and Reverse Tracing

Cryptocurrency investigations can move in two directions. Forward tracing follows funds from victim to criminal, maintaining direct connections suitable for asset recovery and prosecution. Reverse tracing works backward from known criminal infrastructure to identify funding sources.

The B.A.T.S. framework serves both criminal investigators and AML/CTF professionals by recognizing that both groups employ identical methodologies, merely entering the investigative cycle at different points. Criminal investigators typically begin with victim reports (RED wallets) and trace forward to discover criminal infrastructure. AML/CTF professionals often begin with known criminal infrastructure (sanctioned addresses, suspicious activity) and trace backward to identify exposure and potential victims.

Unified Framework for Criminal and AML/CTF Investigations

Both groups utilize the same wallet classification system, with RED wallets always representing victim-facing addresses where funds were criminally obtained. When AML investigations identify criminal infrastructure, these are classified according to their function (YELLOW for hub wallets, PURPLE for exchanges, etc.) rather than creating new categories. This unified approach ensures seamless handoffs between compliance teams and law enforcement.

Backward Discovery Within Forward Focused Investigations

During Level 3 and 4 investigations, investigators frequently encounter terminal wallets (typically exchanges) containing significantly more funds than their traced thread values. When a thread of $50,000 enters an exchange wallet holding $1,000,000, investigators must make a diligent effort to determine the source of the remaining $950,000 to maximize asset recovery opportunities and exhibit criminal intent.

This backward discovery process operates as an embedded Level 1 exercise within the higher-level investigation. Investigators work backward from the terminal wallet using rapid assessment techniques to identify potential additional criminal sources or victims. This backward phase prioritizes speed over documentation precision - investigators are seeking new starting points rather than building evidentiary trails.

Once potential RED wallets or criminal sources are identified upstream, investigators transition back to forward tracing from these newly discovered origins. This creates a natural investigative rhythm: backward for discovery, forward for documentation. Hop counting and meticulous documentation only apply during the forward phase.

The Four Investigation Levels: Matching Method to Purpose

Every cryptocurrency investigation falls into one of four categories based on what you're trying to accomplish. Each level builds on the previous one, but you don't always need to progress through all four. The level you choose depends on your case goals and available resources.

Level 1: Discovery
Level 2: Intelligence
Level 3: Case Preparation
Level 4: Asset Forfeiture

Level 1: Discovery - Getting Your Bearings

Purpose: Quick assessment and lead generation
When to use: Initial case evaluation, understanding scope, finding leads

Discovery analysis focuses on exploration over documentation. You're following interesting patterns to see where they lead, making go/no-go decisions about case priority, and identifying potential for deeper investigation.

What You're Looking For:

- Exchange Connections: Wallets that send funds to known cryptocurrency exchanges represent potential cash-out points
- Obvious Timing Patterns: Multiple wallets moving funds at similar times establishing patterns of activity can show concerted efforts or provide clues on geographical location.
- Shared Infrastructure: Different parts of your investigation using the same mixing services, bridges, or tools indicating common operational patterns
- Large Hub Wallets: Addresses that appear to receive from multiple identified or suspected victim sources

Documentation Standards:
Minimal formal documentation

- Essential screenshots of key transactions and patterns
- Quick notes in whatever format works: "Victim → 3 hops → HTX deposit"
- Rough estimates: "~$50K root total, ~$30K to Binance"
- Key observations: "small amounts moving regularly to Cash App"

End-of-Discovery Summary (5 minutes maximum):
Worth pursuing? [Yes/No]
Estimated scope: [Small/Medium/Large operation]
Key destinations: [Exchange names or services]
Obvious patterns: [One-line description]
Recommended next level: [Intelligence/Case Prep/Asset Forfeiture]
Time invested: [minutes]

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

What NOT to Document: Transaction hashes, precise amounts, formal wallet classifications, detailed timing analysis, or mathematical accounting. Discovery is about speed and intuition - save the precision for higher levels.

Time Investment: 10-60 minutes
Example: You receive a complaint about a romance scam where a victim lost $25,000 in Bitcoin. During your initial analysis, you need to quickly assess whether this case warrants deeper investigation. You trace the victim's funds through several transactions and discover that they eventually arrive at a wallet that has previously received funds from known Lazarus Group infrastructure. Additionally, you notice that the transaction amounts and timing patterns match indicators from a recent FinCEN advisory about North Korean cryptocurrency theft operations.

This discovery phase analysis, completed in minutes, immediately elevates the case priority and triggers notifications to relevant sanctions enforcement teams. The pattern recognition during discovery suggests this isn't an isolated romance scam but potentially part of a larger DPRK-affiliated operation targeting multiple victims.

Limitations: Discovery creates leads and intelligence, not court-ready evidence. However, discovery gives you the most information per hour invested and helps you decide whether deeper analysis is worthwhile.

For AML/CTF Professionals:

The same decision framework applies when assessing suspicious activity:

Start with Regulatory Requirements:

- Below SAR thresholds? Level 1 discovery may suffice for risk assessment
- Meets SAR filing requirements? Level 2 intelligence development needed
- Law enforcement requesting support? Level 3 case preparation standards apply

Consider Risk Exposure:

- Direct exposure (0-1 hops from known bad)? Higher level analysis warranted
- Indirect exposure (2-3 hops)? Level 1-2 may be sufficient
- Distant exposure (4+ hops)? Document and monitor

Plan for Case Evolution
Many cases start at one level and evolve to require higher levels of analysis. A case might:

1. Begin as Level 1 discovery to assess scope
2. Develop into Level 2 intelligence development as patterns emerge
3. Progress to Level 3 case preparation when suspects are identified
4. Finally require Level 4 asset forfeiture analysis when seizure opportunities arise

Design your documentation to support this evolution. Even during initial discovery, maintain standards that will allow you to escalate your analysis if circumstances change. The wallet numbering system must remain stable and permanent once established in Level 2 - wallet IDs assigned never change when transitioning between levels.

Level 2: Intelligence Development - Understanding Criminal Operations

Purpose: Wallet behavior analysis and network mapping
When to use: Understanding how criminal operations work, preparing for complex investigations.

Intelligence development helps you understand criminal network structure and operational methodology. The focus shifts from following specific victim funds to analyzing how wallets behave, and criminal networks operate.

RED Wallet Index Creation: This is where you create the first formal wallet index - the RED wallet index. Each victim-facing wallet gets assigned a formal identifier (R1, R2, R3, etc.) that will remain permanent throughout the investigation. This index serves as the foundation for all subsequent analysis.

Network Behavior Description: Beyond the RED wallet index, describe wallet behaviors without assigning formal IDs. For example: "The network employs 20 intermediary wallets before converging at a hub wallet" rather than naming each individual wallet. Formal ID assignment for non-RED wallets occurs later when creating the universal wallet index.

Key Investigation Techniques:

- Gas Fee Analysis: When criminals operate multiple wallets, they may pay transaction fees from a single funding source - identifying these patterns proves common control
- Network Structure Mapping: Document how RED wallets interact with intermediary wallets and convergence points
- Behavioral Pattern Recognition: Operational timing windows, amount preferences, infrastructure choices
- Hub Wallet Analysis: Identify where funds from multiple victims converge, proving common criminal control
- Infrastructure Analysis: Map preferred exchanges, mixing services, and money laundering tools
- Back-tracing: identification of other potential funding sources/exposure to VASPs or additional potential victims
- Cluster Analysis: looking for exposure to known entities through other wallets associated to wallets in your investigation but with no exposure to your specific crime
- The 80% Rule: Follow major money movements to understand operational methodology without mathematical precision. You're studying wallet behaviors, not accounting for every dollar of victim funds.

Network behavior analysis focuses on identifying patterns of use that characterize money laundering operations. Courts have recognized that examining patterns of use - such as accounts repeatedly receiving and moving criminal proceeds - can establish the systematic nature of criminal operations. This behavioral analysis serves both intelligence development and supports various legal theories in subsequent proceedings.

Network Analysis Example:

RED WALLET INVENTORY:
R1: 15,000 USDT (romance scam victim)
R2: 30,000 USDT (investment fraud victim)
R3: 12,000 USDT (recovery scam victim)
Total: 57,000 USDT across 3 victims

NETWORK STRUCTURE:
- RED wallets (3 total) interacted with 20 intermediary wallets
- Convergence point: Hub wallet where R1, R2, R3 funds commingled
- Infrastructure: FixedFloat bridge to Tron network
- Terminal: Binance deposits totaling ~57,000 USDT between [date range]

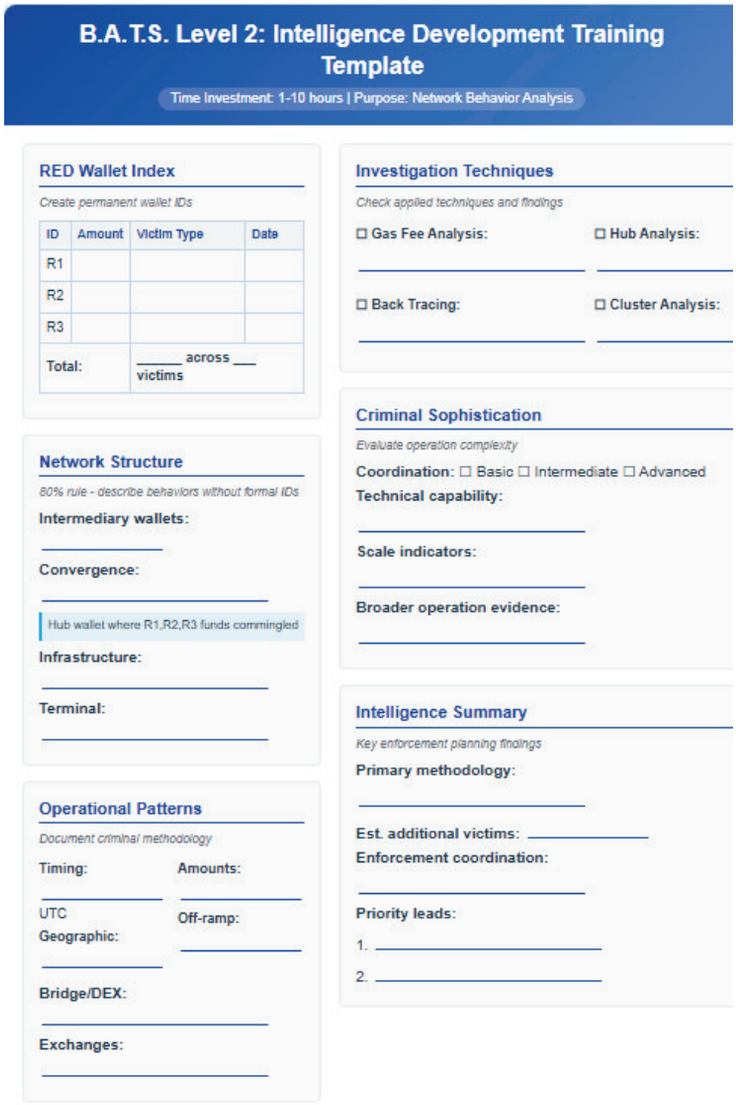
OPERATIONAL PATTERNS:
- Timing: 2-6 AM UTC operational window
- Bridge methodology: Consistent use of FixedFloat
- Off-Ramping behavior: Large consolidated Binance deposits
- Amount preferences: Round USD equivalents

CRIMINAL SOPHISTICATION:
- Multi-victim convergence demonstrates coordinated operation
- Cross-chain laundering indicates intermediate technical capability
- Large-scale cash-out suggests established exchange relationships

Time Investment: 1-8 hours
Example: Building on the romance scam case from Level 1, you now need to understand the broader criminal network structure. Your analysis reveals that the operation uses a consistent pattern: victims' funds are first converted to USDT through decentralized exchanges, then bridged to the Tron network where they're consolidated into hub wallets. The timing analysis shows that these conversions consistently occur between 2:00-6:00 AM UTC, suggesting operational control from a specific geographic region.

Further network mapping reveals that this criminal organization shows a strong preference for using FixedFloat for initial conversions and HTX exchange for final cash-outs. The same operational patterns appear across multiple victim types - romance scams, fake investment platforms, and crypto recovery scams - all using identical money laundering infrastructure. This intelligence development reveals that what appeared to be separate criminal schemes are actually different initiatives for the same organized operation.

Your analysis documents over 200 connected wallets, identifies the preferred geographic operating window, and maps the complete money laundering methodology. This intelligence product enables law enforcement to understand the full scope of the criminal enterprise and plan coordinated enforcement actions across multiple schemes.



Level 3: Case Preparation - Building Evidence for Court

Purpose: Creating prosecution-ready evidence and pursuing records through legal process
When to use: Supporting criminal charges, search warrant applications, court proceedings

Case preparation creates documentation suitable for criminal prosecution using wallet-centric investigation methodology. You're building evidence chains through the criminal network that prosecutors can present to judges and juries. At this stage you need to apply consistent PIFO or LIBR methodology with matching transactions where appropriate and document decisions in trace paths.

Universal Wallet Index: At this level, create a comprehensive index of all wallets involved in the money laundering process, assigning permanent IDs that will never change throughout the investigation. This expands beyond the RED wallet index to include all wallet types with formal notation.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

V-T Notation System: Victim-Transaction notation tracks evidence chains through criminal networks

- V = Victim number
- T = Transaction sequence
- Example: V1-T1 (Victim 1, Transaction 1,)

TRACE V1-T1:
V1-T1 / R1 (RED-1):
Received: .34 BTC from victim on 1/15/25 14:30 UTC
TxID: a1b2c3d4e5f6...
Notes: Wallet R1 had 13 separate UTXOs representing 1.3 BTC prior to this transfer. The .34 BTC subject to this trace was sent to wallet B7 as an aggregate of smaller UTXOs representing a total transfer of .41 BTC but was determined to be the target thread value under PIFO method.

V1-T1 / B7 (BLACK-7):
Received: .41 BTC on 1/15/25 14:45 UTC
TxID: f6e5d4c3b2a1...
Notes: Wallet B7 had no other activity and was only used to receive the assets from R1 and move them to P3

V1-T1 / P3 (PURPLE-3): - HTX DEPOSIT
Received: .41 BTC on 1/15/25 15:00 UTC
TxID: 1f2e3d4c5b6a...
Exchange: HTX confirmed via deposit address clustering
Notes: Letterhead sent for records

Note on Embedded Discovery Within Higher-Level Investigations
Level 3 and 4 investigations frequently require embedded Level 1 discovery exercises when terminal wallets contain funds exceeding traced amounts. Investigators should:

- Document their primary thread to completion
- Conduct rapid backward discovery to identify additional sources
- Create new forward traces from discovered sources
- Maintain separate V-T references for each distinct victim/source identified

This iterative process maximizes asset recovery while maintaining documentation integrity.

Documentation Requirements
Your work needs to:

- Clearly connect technical evidence to criminal behavior
- Use language that non-technical audiences can understand
- Focus on legally significant transactions
- Provide sufficient detail for other experts to verify your conclusions

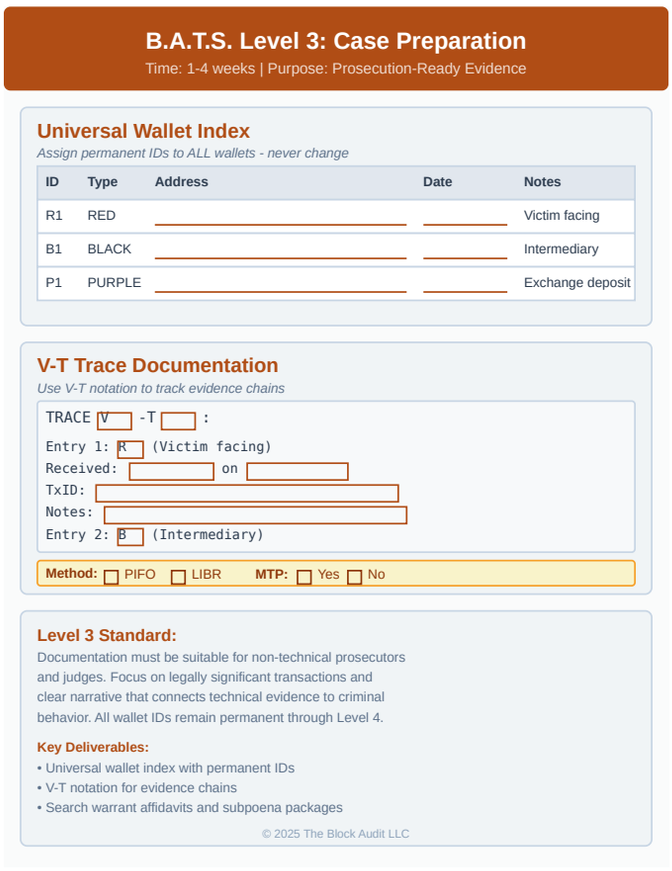
Legal Narrative Development: Use the above noted transaction information to connect technical findings to criminal behavior prosecutors need to prove. Don't just show that funds moved from wallet A to wallet B - explain what that movement means for the criminal case and what a reasonable investigator can infer based on training and experience from the behaviors recognized.

Time Investment: 1-5 days

Example: Your intelligence development from Level 2 has identified specific VASPs where the criminal network consistently cashes out: HTX, KuCoin, and several smaller exchanges. Now you need to build evidence supporting subpoenas for these institutions to obtain KYC records and internal transaction logs. Your case preparation analysis focuses on demonstrating clear connections between the criminal network and specific exchange deposit addresses.

You document that deposits to HTX account address bc1q...xyz can be directly traced to 17 different victim transactions totaling $890,000 over six months. Your analysis shows that internal HTX records will reveal account ownership, deposit patterns, and withdrawal methods that can identify the criminal operators or location of stolen assets. You prepare detailed transaction flow charts showing how victim funds moved through the money laundering network to reach specific exchange accounts.

The documentation includes professional-grade evidence suitable for warrant applications, with clear narrative explanations that non-technical prosecutors and judges can follow. Your analysis demonstrates not only that criminal proceeds reached specific exchange accounts, but also that obtaining these records will provide actionable intelligence for arrests and additional asset recovery. The case preparation creates a foundation for search warrants, extradition requests, and coordination with international law enforcement partners.



Training Templates available upon request

Level 4: Asset Forfeiture - Mathematical Precision for Seizures

Purpose: Maintaining golden thread for asset recovery
When to use: Preparing to seize cryptocurrency assets

Asset forfeiture represents the most demanding level of cryptocurrency investigation from both a legal as well as ethical perspective. When you're preparing to seize someone's cryptocurrency, it is incumbent on you to perform your analysis in a conservative and defensible manner. Courts require proof that seized assets are "directly traceable" to criminal activity, and defense attorneys will challenge every aspect of your methodology.

The Critical Transition: Why Level 4 Requires Different Thinking

The Legal Problem Level 4 Solves

The transition from Level 3 to Level 4 represents a fundamental conceptual shift that many investigators initially struggle to understand. This shift is crucial because Level 3 and Level 4 solve different legal problems:

Level 3 can prove: "These funds came from the victim and ended up in this wallet"
Level 4 can prove: "These specific assets in this wallet are the exact same dollars/assets stolen from the victim"

This distinction becomes critical when defense attorneys argue:

- "Yes, criminal money passed through this wallet, but the funds you're seizing came from legitimate sources that also used this wallet"
- "You can't prove which specific dollars in this mixed wallet represent criminal proceeds"
- "The commingling broke the direct connection - these could be anyone's funds"
-

Level 3 puts criminals in jail when they can be located, which is rare. Level 4 gets victims their money back and commits excess criminal proceeds to the fight against criminal networks through increased resources by asset forfeiture efforts, rather than sending excess proceeds back into the criminals.

Level 3 gives you a prosecution case but might lose asset forfeiture challenges. Level 4 gives you the mathematical precision to survive those challenges and seize entire accounts.

Conceptual Framework Shift

Levels 1-3: Wallet-Centric Investigation

- Following wallets through the network
- V-T notation tracks "which wallet appears where in the sequence"
- Goal: Understanding criminal network structure and evidence chains

Level 4: Transaction-Centric (Hop) Investigation

- Following specific dollar amounts through mathematical hops
- V-T-H notation tracks "how far these specific funds have traveled"
- Goal: Maintaining golden thread for asset forfeiture

The fundamental difference:

- V-T: "Victim 1's first transaction reached wallet BLACK-7 as the third wallet in the sequence"
- V-T-H: "Victim 1's first transaction is now 3 hops away from the original crime"

It's like the difference between mapping a road network (which cities connect to which) versus calculating travel distance (how far you've gone from your starting point). Same underlying network, completely different analytical frameworks serving different legal purposes.

B.A.T.S. Level 4 Methodology

V-T-H Notation System and Hop Counting

B.A.T.S.'s standardized identification system employs ***V-T-H notation***, where V represents the victim number, T represents the transaction number from that victim, and H represents the hop count from the victim facing wallet. This notation enables clear communication between investigators and provides precise identification of any trace path within complex multi-victim investigations.

Hop counting measures the distance from the victim facing wallet rather than chronological discovery order. Each blockchain transaction increments the hop count by one, regardless of when investigators discover the transaction during their analysis. This distance-based approach ensures consistent documentation and enables mathematical validation of trace completeness.

Core Amount Classifications

B.A.T.S. employs a three-tier system for tracking monetary amounts throughout an investigation:

Root: The original amount of a victim's transaction that forms the baseline for all subsequent tracing. This amount serves as the starting point for accounting validation and cannot be exceeded by traced amounts at any point in the investigation.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

***Adjusted Root Total* (ART):** Accounts for practical investigation limitations by subtracting documented write-offs from the root total. Write-offs include dust amounts below investigation thresholds, traces that become too diluted to pursue practically, assets entering obfuscation services, or paths abandoned due to operational constraints. All write-offs must be documented with justification to maintain investigative integrity.

***Thread*:** The specific amount being traced at any given point in the investigation. Unlike the root total, which remains constant, thread totals change as funds split, merge, or encounter partial outflows during their movement through the blockchain.

Convergence and the Sequential Hop Rule
Complex cryptocurrency investigations inevitably encounter convergence scenarios where multiple trace paths arrive at the same wallet before moving out together as a single transaction. The *Sequential Hop Rule* resolves convergence by applying the highest hop count among all converging paths, plus one for the outbound transaction.

For example, if paths arriving at a hub wallet have hop counts of H2, H4, and H6, the outbound transaction becomes H7 (6+1). This conservative approach ensures that seized assets can be proven to have traveled at most the maximum distance from any original crime.

Convergence creates natural reset points where previously separate paths combine into single outbound flows. From the convergence point forward, all converged funds move together with identical hop counts, simplifying subsequent tracking while maintaining individual victim accounting.

Accounting Validation and Mathematical Integrity
B.A.T.S.'s most innovative feature is its built-in mathematical validation system that ensures investigative completeness and prevents scope creep. This fundamental accounting principle requires that all thread totals at any given hop level must sum to the adjusted root total.

This validation provides multiple benefits. First, it serves as a completeness check - if thread totals at a given hop level don't sum to the adjusted root total, investigators know they've missed trace paths. Second, it prevents scope inflation by maintaining strict mathematical boundaries around traced amounts. Third, it provides courtroom-ready evidence demonstrating that every dollar has been accounted for throughout the investigation.

Practical Validation Process: Investigators implement ***root validation*** by summing all thread totals sharing the same hop count and comparing this sum to the adjusted root total. For example, if V1-T1 has an adjusted root total of $9,500 after $500 in write-offs, then all V1-T1-H2 entries must sum to $9,500, all V1-T1-H3 entries must sum to $9,500, and so forth. Discrepancies immediately identify investigation gaps. If H3 thread totals sum to only $8,200, investigators know $1,300 in trace paths remain undiscovered. This mathematical precision eliminates guesswork from complex investigations.

Write-off Management and Scope Control
Real-world investigations encounter practical limitations requiring documented abandonment of certain trace paths. B.A.T.S. acknowledges these realities through systematic *write-off* procedures that maintain accounting integrity while recognizing investigation constraints.

Dust write-offs handle transactions below practical investigation thresholds, typically under $50 but subjective to the investigation. Dilution write-offs address scenarios where thread totals become impractically small percentages of larger transactions, such as following $50 of a $10,000 movement. Obfuscation write-offs account for assets entering mixing services, privacy coins, or other technologies that effectively terminate traceability. Operational write-offs recognize resource limitations when investigations would require pursuing dozens of micro-transactions or other impractical trace paths.

Each write-off requires documentation specifying the amount abandoned, hop level where abandonment occurred, write-off category, and brief justification. These documented write-offs adjust the root total downward, creating a new adjusted root total that becomes the target for subsequent accounting validation.

Multi-Victim Investigation Management
B.A.T.S.'s hierarchical structure naturally accommodates complex investigations involving multiple victims whose funds flow through shared criminal infrastructure. The V-T-H notation system enables separate accounting for each victim while tracking convergence points that prove common criminal control.

When multiple victims' funds converge at hub wallets, investigators can demonstrate the scope of criminal operations while maintaining individual victim accounting for asset recovery purposes. Merged notation using formats like V1,V2-T1-H3 documents convergence while preserving the ability to calculate individual victim losses and recoveries.

Multi-victim investigations benefit particularly from B.A.T.S.'s accounting validation, as investigators must balance multiple root totals simultaneously. The mathematical precision prevents one victim's investigation from inadvertently expanding into another victim's traced funds.

B.A.T.S. Standard Reporting Format

Professional cryptocurrency investigations require standardized documentation that serves multiple audiences – from technical investigators to prosecutors, judges, and juries. B.A.T.S. establishes a comprehensive reporting format that transforms complex blockchain analysis into accessible, legally compelling evidence packages. This standardized approach ensures consistency across investigation teams while providing complete audit trails for legal proceedings. This process also seeks to document all information for an independent investigator to audit and verify any portion of the trace so that they do not need to put blind faith into the final work product provided by another investigator/analyst.

Section 1: Case Summary
The report begins with a concise case summary that establishes the criminal context and scope of the investigation. This section identifies the type of fraud or criminal activity, the timeframe of the scheme, and the total number of victims affected. The summary provides essential context for understanding why the subsequent technical analysis matters for the case.

Section 2: Wallet Indices
In order to streamline documentation, the report starts with various indices to summarize victim deposits, total losses, date ranges, known criminal wallets, and a reference to substitute full wallet addresses with wallet IDs in compliance with the B.A.T.S. wallet classification system. This section includes a transaction index, victim facing wallet index, and a universal wallet index.

Victim Transaction Index: A transaction index follows immediately, providing a clear overview of each victim's participation in the scheme and their financial losses. This section employs a standardized victim table format consisting of Transaction number, loss amount (root total), USD equivalent, date, and notes.

Victim 1 INDEX

Trans #	Loss Amount	USDe	Date	Notes
1	3.2 BTC	320,000	1/1/25	Investment
2	3,050 USDT	3,050	1/15/25	Fee Payment
3	1.023 BTC	110,000	1/20/25	Taxes

Victim 2 INDEX

Tran #	Loss Amount	Approx USD	Date	Notes
1	.02 BTC	2,000	1/15/25	Test Investment
2	8,050 USDT	8,050	1/25/25	Full Investment

Victim Facing Wallet (RED) Index: The victim facing wallet index provides a visual summary of how victim funds initially entered the criminal infrastructure, serving as a crucial reference for understanding the scope and organization of the criminal operation. This index employs a standardized format that immediately communicates the scope of the investigation and existing investigative leads.

RED WALLET INDEX

Wallet ID	Wallet Address	Victim Transactions	Notes
RED-1	1A1zP1eP5QGefi7rwywhjDivfNayjryh	V1-T1 V1-T2 V2- T1	Provided by "Billy" via WhatsApp
RED-2	3J98t1WpEZ73hgkf7oIRhWNLyr34yyjje	V1-T3 V2-T2	

Universal Wallet Index: The comprehensive wallet index serves as the investigation's technical appendix, providing complete wallet identification and address mapping for all wallets involved in the money laundering process. This index enables technical verification of the investigation while maintaining documentation clarity by keeping lengthy wallet addresses separate from the main analytical narrative.

The wallet index employs a standardized classification structure that groups wallets by their B.A.T.S. color classifications. It consists of columns for the Wallet ID Classification, the full wallet address, the first appearance, and notes.

Section 3: Trace Documentation
Purpose: Document every traced transaction to enable independent verification. Each entry must contain sufficient detail for audit and reproduction.

Step 1: Create the Entry Header
Use V-T-H notation to identify the transaction:
[V#-T#-H#]
Adjusted Root Total (ART)
EX) V1-T2-H3, 3000 USDT

Step 2: Record Transaction Details
Source Wallet ID → Destination Wallet ID
Transaction Hash
Date/Time Stamp
Thread Total / Adjusted Root Total

EX)
BLACK 2 > BLACK 3
0xmfl6k6dfddpdigjgpo6o5y8f2a3b4c5d6e7f8g9h0i1j2k3l4g5t
1/1/25 3:05 AM UTC
1500 USDT/3000 USDT

BLACK 2 > BLACK 4
PnipoIHblefmiMtlijgoie98y4oi3k8f0936lV4Jblkdlsnldksldjeo7
2/3/25 12:56 AM UTC
500 USDT/3000 USDT

BLACK 2 > GRAY 1
TH803nvF9jlefninenmLHbGjkvLLl69vbuf74N4Jblkdlsnldksldje
2/5/25 4:23 PM UTC
1000 USDT/3000 USDT

Step 3: Notes
Include these details in a narrative format:

- Beginning adjusted root total (ART)
- Summary of all outgoing transactions by wallet classification
- Explanation of wallet functions (i.e. wallet Brown 1 was used to convert 1000 USDT into 998 USDC)
- Write-offs

Any deviations to PIFO require explanation.

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

EX) V1-T1-H3 had a beginning ART of 3000 USDT. These assets were split between 3 receiving wallets: BLACK 3, BLACK 4, and GRAY 1. A total of 2000 USDT entered BLACK wallets and continued in the money laundering network to V1-T1-H4. The 1000 USDT entering GRAY 1 was abandoned due to effective obfuscation

Step 4: Root Validation

Verify that all traced thread values add up to the ART to ensure accuracy and integrity of the trace.

EX)

Beginning ART 3,000 USDT
Traced Assets -2,000 USDT
Abandoned Assets -1,000 USDT

Step 5: Adjusted Root Total

After conducting your root validation clearly state the new ART which will be referenced for future hops.

EX) Adjusted Root Total (ART) = 2000 USDT

Section 4: Summary of Findings

Purpose: Provide a concise narrative summary of the investigation and create an actionable index for continued investigation and asset recovery efforts.

Investigation Summary: Write a narrative summary covering these key elements:

Money Laundering Network Analysis

- Wallet Count: Total number of wallets involved in the laundering process
- Obfuscation Techniques: Specific methods used (mixing services, privacy coins, chain hopping, etc.)
- Criminal Infrastructure: Hub wallets, conversion points, timing patterns

Victim Impact and Scope

- Confirmed Victims: Number of victims traced in current investigation
- Additional Victims Identified: Potential victims discovered but not traced
- Scope Expansion Opportunities: Recommendations for broadening investigation
- Criminal Organization Scale: Evidence of broader criminal operation

Terminal Point Analysis

- Asset Distribution: Where traced funds ultimately terminated
- Golden Thread Verification: Confirmed amounts traceable to original crimes
- Recovery Prospects: Realistic assessment of asset recovery potential

Example Narrative: *"Investigation revealed a sophisticated money laundering network utilizing 47 wallets across 6 blockchain hops. The criminal operation employed advanced obfuscation techniques including Tornado Cash mixing, cross-chain bridges, and privacy coin conversions. Analysis identified 3 confirmed victims with $45,000 in traced losses, plus evidence of 7 additional potential victims requiring scope expansion consideration. $38,000 (38%) of the Root $100,000 (initial loss) was traced to 4 separate exchange deposit addresses with potential for additional records, suspect identification, or asset recovery."*

Exchange Records Index: An exchange records index is intended to be a snapshot summary of all assets successfully traced to identifiable exchanges to facilitate and expedite the pursuit of exchange records and asset recovery. This index communicates the specific exchange deposit addresses which received funds directly traceable to specific victim transactions as well as a total of all assets entering the wallets that are directly traceable to criminal activity.

Wallet ID	Wallet Address	Exchange	Victim Transactions	Thread Total
Purple 1	bc1dHlfgK74FTykvs56F43kl563dGRds45964Dfh5	Binance	V1-T2,T3,T5	1.2 BTC
Purple 2	0x5Lui4DfgK74FTykfki7533dPh51Srg4T789GdF2G	Coinbase	V1-T1,T4,T6	15,670 USDT

Conclusion

Effective cryptocurrency investigation starts with choosing the right approach for your goals. Not every case needs the mathematical precision required for asset seizures, and not every lead-generation effort needs the detailed documentation required for prosecution.

Understanding these four levels - discovery, intelligence development, case preparation, and asset forfeiture - helps you allocate your time and resources effectively. Start with your objectives, consider your constraints, and choose the approach that best serves your needs.

Remember that cases often evolve from simple discovery to complex asset forfeiture investigations. Maintaining good documentation standards from the beginning ensures you can escalate your analysis when opportunities arise.

The Block Audit Tracing Standard represents the highest standard of cryptocurrency investigation, most valuable when you understand exactly when and why this level of precision becomes necessary. By following this comprehensive framework, investigators can maintain the golden thread of traceability while building legally sound evidence that withstands judicial scrutiny and enables successful victim asset recovery.

B.A.T.S. Investigation Workflow

B.A.T.S. LEVELS 1-3 (CONTEXT)

1 Discovery (10-60 min)
Quick assessment and patterns
Go/no-go decision

2 Intelligence (1-40 hrs)
RED wallet index
Network mapping

3 Case Prep (1-4 weeks)
Universal wallet index
Court-ready evidence

LEVEL 4: ASSET FORFEITURE (1-6 months) - 7 STEP PROCESS

1 Establish Root Total and Classification

- Document V1-T1 with exact amount
- Mark receiving wallet as RED
- Establish root total baseline

2 Begin Hop Counting and V-T-H Notation

- V1-T1-H1: First movement from RED wallet
- Specify exact thread total being traced
- Hop count = distance from crime

3 5-Step Documentation Process

Step 1: V-T-H notation with ART
Step 2: Wallet IDs, hash, timestamp
Step 3: Narrative notes and PIFO deviations
Step 4: Root validation
Step 5: Update ART and available threads

4 Sequential Hop Rule and Convergence

- Mark convergence wallets as YELLOW
- Outbound hop = MAX(incoming) + 1
- Document convergence in narrative

5 Write-offs and Adjusted Root Total

- Categories: Dust, dilution, obfuscation, operational
- Document amount, hop level, justification
- New ART = Root Total - Write-offs

6 Continuous Root Validation

Thread Totals at H[n] = Adjusted Root Total

- Verify traced + abandoned = ART at each hop
- Calculate new ART after write-offs

7 Complete Investigation and Generate B.A.T.S. Report

Section 1	Section 2	Section 3	Section 4
Case Summary	All Indices	Trace Documentation	Summary of Findings

© 2025 The Block Audit LLC - www.theblockaudit.com

B.A.T.S. Level 1: Discovery Training Template

Time Investment: 10-60 minutes | Purpose: Quick Assessment

Case Information

Fill in basic case details

Case #: _____

Investigator: _____

Victim:

_____

Loss: $ _____ in

_____

Date: _____ **Start Time:**

_____

Initial Observations

Document rapid assessment findings

Payment Address:

_____

Flow Pattern:

_____

> **Example:** "Victim → 3 hops → HTX deposit"

Est. Traced: ~$ _____

Terminal:

_____

Pattern Recognition

Check observed patterns

- ☐ Exchange: _____
- ☐ Timing: _____
- ☐ Infrastructure: _____
- ☐ Hub activity: _____
- ☐ Sanctions: _____

Key Screenshots

List essential captures

1. _____
2. _____
3. _____
4. _____
5. _____

Additional Observations

Note any significant findings

_____

_____

_____

_____

_____

_____

Time Tracking

Completed in: _____ minutes

Target: 10-60 minutes

End-of-Discovery Summary (5 minutes max)

Worth pursuing?

☐ Yes ☐ No

Estimated scope:

☐ Small ☐ Medium ☐ Large

Next level:

☐ Intel ☐ Prep ☐ Forfeiture

Key destinations: _____

Obvious patterns: _____

B.A.T.S. Level 2: Intelligence Development Training Template

Time Investment: 1-10 hours | Purpose: Network Behavior Analysis

RED Wallet Index

Create permanent wallet IDs

ID	Amount	Victim Type	Date
R1			
R2			
R3			
Total:	_____ across ___ victims		

Network Structure

80% rule - describe behaviors without formal IDs

Intermediary wallets:

_____

Convergence:

_____

> Hub wallet where R1,R2,R3 funds commingled

Infrastructure:

_____

Terminal:

_____

Operational Patterns

Document criminal methodology

Timing: _____ UTC

Amounts: _____

Geographic: _____

Off-ramp: _____

Bridge/DEX:

_____

Exchanges:

_____

Investigation Techniques

Check applied techniques and findings

☐ **Gas Fee Analysis:** _____

☐ **Hub Analysis:** _____

☐ **Back Tracing:** _____

☐ **Cluster Analysis:** _____

Criminal Sophistication

Evaluate operation complexity

Coordination: ☐ Basic ☐ Intermediate ☐ Advanced

Technical capability:

_____

Scale indicators:

_____

Broader operation evidence:

_____

Intelligence Summary

Key enforcement planning findings

Primary methodology:

_____

Est. additional victims: _____

Enforcement coordination:

_____

Priority leads:

1. _____
2. _____

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

B.A.T.S. Level 3: Case Preparation Training Template

Time Investment: 1-5 days | Purpose: Prosecution-Ready Evidence

Universal Wallet Index Creation

Assign permanent IDs to ALL wallets - these will never change throughout investigation

Wallet ID	Classification	Full Address	First Appearance	Notes
R1	RED	_____	_____	Victim facing
B1	BLACK	_____	_____	Intermediary
P1	PURPLE	_____	_____	Exchange deposit

V-T Trace Documentation

Use V-T notation to track evidence chains. Apply consistent PIFO or LIBR methodology.

```
TRACE V_____-T_____:
Entry 1: R_____ (Victim facing wallet) Received: _____ from victim on _____
TxID: _____
Notes: _____
_____
Entry 2: B_____ (Intermediary wallet) Received: _____ on _____
TxID: _____
Notes: _____
_____
```

Methodology Documentation

Document tracing method and justify deviations

Method: ☐ PIFO ☐ LIBR | **MTP:** ☐ Yes ☐ No

Justification: _____

B.A.T.S. Level 4: Asset Forfeiture Training Template

Time Investment: 1-2 weeks | Purpose: Mathematical Precision for Seizures

CRITICAL: Level 4 requires conservative, defensible analysis. Demonstrate specific assets in seized wallets came from specific criminal acts with mathematical certainty.

Root Total

Establish baseline for mathematical validation

Victim: V_____
V1

Original Loss: _____
5000

Date: _____
1/1/25 / 1800 UTC

Transaction: T_____
T2

Asset Type: _____
USDT

Starting Hop: H1

Root Total = _____ *5000 USDT*

Hop Documentation

Document each hop with mathematical precision

ADJUSTED ROOT TOTAL (ART): _____ *5000 USDT*

V_____-T_____-H_____ *V1-T2-H2*

_____ → _____ | Thread Total: _____
Red 1 → Black 1 | Thread Total: 2000

Date: | **Time:** | **TZ:** _____
Date: 1/1/25 | Time: 1800 | TZ: UTC

TxID: _____

PIFO: ☐ Yes ☐ No ☐ MTP | Notes: _____

V_____-T_____-H_____ *V1-T2-H3*

_____ → _____ | Thread Total: _____
Black 1 → Purple 1 | Thread Total: 1000

Date: | **Time:** | **TZ:** _____

TxID: _____

PIFO: ☐ Yes ☐ No ☐ MTP | Notes: _____

VALIDATION: _____ + _____ = _____ | Root: _____ - Traced: _____ = Unaccounted: _____

 © 2025 The Block Audit LLC. All Rights Reserved. Proprietary Process.

Root Validation Process

Mathematical verification - all thread totals at each hop level must sum to adjusted root total

Hop Level	Thread Totals	Sum	ART	✓/✗
H2	_____ + _____	_____	_____	_____
H3	_____ + _____	_____	_____	_____

Validation Check: If sums don't equal ART, you've missed trace paths. Discrepancies = investigation gaps.

Write-off Documentation

Document any abandoned trace paths with justification

Amount	Hop	Category	Justification
_____	H_____	☐ Dust ☐ Dilution ☐ Obfuscation	_____
_____	H_____	☐ Dust ☐ Dilution ☐ Obfuscation	_____

ART Calculation: Original: _____ - Write-offs: _____ **= New ART:** _____

Convergence Documentation

Apply Sequential Hop Rule when multiple paths converge

Converging Paths:

Path 1: H_____ (_____) | Path 2: H_____ (_____)

Sequential Hop Rule: Highest incoming hop: H_____ + 1 = **Outbound hop:** H_____

Merged Notation: V_____,V_____-T_____-H_____

Golden Thread Verification

Confirm unbroken mathematical connection from victim to seizure target

Final Traceable Amount (Golden Thread):

_____

Target Asset Location:

_____

Legal Standard: Demonstrate these specific assets are directly traceable to the original crime with mathematical certainty.

MORE INFORMATION

www.TheBlockAudit.com

The procedures outlined in this guide were developed by the owners of The Block Audit LLC; Alex Arenas and Jesse Gossman, who have nearly 40 years of combined law enforcement experience between the Fort Lauderdale Police Department and the Manhattan District Attorney's Office, where they have spent most of their careers dedicated to emerging financial crimes. Thier combined education and training includes a master's degree in forensic accounting, designations as Certified Fraud Examiners, and a host of other crypto and fraud specific certifications. All of this training, education, and experience was used in the formulation of these processes. If you would like training on this method or access to the accompanying web application, you may contact us at:

info@TheBlockAudit.com

or check out

www.BATStool.com

Also check out our other crypto investigation related products at www.TheBlockRecord.com and www.TheBlockService.com or our full service at www.TheBlockAudit.com