[*Placeholder for B.A.T.S. Investigation Workflow Visual*]# A Practitioner's Guide to Crypto Asset Tracing: B.A.T.S Framework Desk Reference

**Introduction: Defining The Investigative Approach**

**Key Terms and Definitions**

**Adjusted Root Total**: The root total minus any documented write-offs. This becomes the accounting baseline that all thread totals must sum to at each hop level for mathematical validation.

**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.

**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.

**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.

**Discovery**: Initial investigation focused on understanding case scope and generating leads rather than mathematical precision.

**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.

**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.

**Intelligence Development**: Systematic analysis focused on understanding criminal network operations and behavioral patterns.

**PIFO Method**: (Proceeds In First Out) - the principle that when traced funds enter a wallet, the very next outbound transaction contains those funds, applied strictly chronologically.

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

**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 Total**: The specific amount being traced at any given hop level. This is the portion of the adjusted root total moving through a particular transaction path.

**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.

**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.

On-Ramping

Off-Ramping

V-T-W Notation

Back Tracing

Cluster Analysis

LIBR Method (Lowest Intermediate Balance Rule)

Matching Transactions Principle (MTP)

Red Wallet index

Universal Wallet Index

B.A.T.S. 1 Discovery

B.A.T.S. 2 Intelligence

B.A.T.S. 3 Case Preparation

B.A.T.S. 4 Asset Forfeiture

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.

**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.

*“Enter a paragraph here on the explanation of pursuing dirty wallets at the terminal point rather than continuous scope creep) throughout.”*

**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 powerful analytical tools.

**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. **Privacy considerations** acknowledge that blockchain analysis can reveal sensitive information about law-abiding individuals.

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. **Conservative interpretation** of unclear legal standards helps avoid precedent-setting conflicts. **Continuous professional development** ensures investigators remain informed about evolving standards. **Active participation** in professional organizations enables contribution to responsible standards development. **Comprehensive documentation** serves multiple purposes beyond individual case requirements.

The cryptocurrency investigation field will be fundamentally shaped by the choices that current practitioners make 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 analytical tools remain available for legitimate law enforcement purposes.

**Universal Standards Across All Levels**

Regardless of which level you choose, 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 detailed analysis for some parts of your investigation and simpler approaches for others, be clear about where you're applying which standards.

**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

**Quality Control**

**Get Second Opinions**: Have other investigators review your key findings  
**Verify Critical Transactions**: Double-check important transactions using multiple blockchain explorers  
**Consider Legal Requirements**: Make sure your methodology will meet the evidentiary standards for your intended use  
**Document Thoroughly**: Keep detailed records of your analytical process and decisions

**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:

**Need to understand the scope?** Start with Level 1 discovery  
**Want to map the criminal network?** Use Level 2 intelligence development  
**Building a prosecution case?** Move to Level 3 case preparation  
**Planning to seize assets?** Use Level 4 asset forfeiture methodology

**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.

**Specialized Investigation Applications**

**Travel Rule Compliance, AML Investigation, and SAR Production**

Travel Rule compliance investigations, Anti-Money Laundering analysis, and Suspicious Activity Report production represent specialized applications that don't correspond directly to the four-tier framework. Instead, these regulatory compliance investigations employ techniques from multiple tiers depending on specific compliance requirements and risk assessment needs.

**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.

**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.

Reverse tracing serves several critical purposes: identifying unreported victims, supporting customer due diligence for financial institutions, and assessing terrorist financing networks. The choice between approaches depends on available information, with sophisticated investigations often using both methodologies.

**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.

Transaction analysis serves asset forfeiture by maintaining mathematical precision necessary for legal proceedings. Cluster analysis supports intelligence development by revealing criminal organization structure and scope.

**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.

**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 directly links all intermediary wallets occurring between the initial RED wallet and the PINK wallet to the criminal network.

**YELLOW wallets**: Hub wallets where multiple victim traces converge. This convergence proves common criminal control and implicates all previous intermediary wallets as part of the criminal network.

**ORANGE wallets**: Bitcoin change addresses essential for UTXO tracing. These technical designations ensure proper accounting in Bitcoin investigations where change addresses can be mistaken for new criminal wallets.

**BROWN wallets**: Handle asset conversion where cryptocurrency types change via bridges, decentralized exchanges, or DApps. These conversions complicate tracing but don't terminate the golden thread.

**BLACK wallets**: Default classification for intermediary wallets with no direct victim exposure. These represent standard money laundering hops without special significance.

**BLUE wallets**: Cold storage – wallets currently holding traced assets. This represents a temporary status that changes when assets move.

**PURPLE wallets**: Exchange deposit addresses where the on-chain trail terminates, and legal process becomes necessary to continue tracing.

**GRAY wallets**: Obfuscated or diluted traces where the path has become effectively untraceable or too diluted to pursue practically.

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

**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]

**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 a 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.

**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 Analysis Template**:

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**: 1-40 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.

**Enhanced Notation System**: [V]-[T]-[W]**V-T-W Notation System**: Victim-Transaction-Wallet notation tracks evidence chains through criminal networks

* V = Victim number
* T = Transaction sequence
* W = Wallet ID from universal index
* Example: V1-T1-B3 (Victim 1, Transaction 1, Black 3 from Universal Wallet Index)

**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, and provide sufficient detail for other experts to verify your conclusi

**Trace Documentation**:

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: $24,900 BTC on 1/15/25 15:00 UTC

├── TxID: 1f2e3d4c5b6a...

├── Exchange: HTX confirmed via deposit address clustering

└── Notes:

**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.

**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.t. 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 dollars in this wallet are the exact same dollars 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. 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-W 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-W**: "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 Total**: 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.

**Adjusted Root Total**: 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 Total**: 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.

**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.

**Matching Transactions Principle**

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.

For example, 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 to UTXO blockchains where specific UTXOs can be traced directly.

**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.

**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**

To streamline documentation, the report includes various indices that summarize victim deposits, total losses, date ranges, known criminal wallets, and reference systems to substitute full wallet addresses with wallet IDs in compliance with the B.A.T.S. wallet classification system.

**Victim Transaction Index**: Provides a clear overview of each victim's participation in the scheme and their financial losses using standardized victim table format consisting of transaction number, loss amount (root total), USD equivalent, date, and notes.

**Victim Facing Wallet (RED) 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.

**Universal 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.

**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  
PnipoIHblefmiMtIijgoie98y4oi3k8f0936lV4JblkdlsnldksIdjeo7  
2/3/25 12:56 AM UTC  
500 USDT/3000 USDT

BLACK 2 > GRAY 1  
TH803nvF9jlefninenmLHbGjkvLLl69vbuf74N4JblkdlsnldksIdje  
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 with explanation  
  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 Total $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.

[*Placeholder for Exchange Records Index Table*]

**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.