

Tracker

*Advanced
Blockchain
Investigations*

FOREWORD

Crypto crime has entered a new phase. Threat actors now use AI-assisted laundering, smart contracts, and cross-chain protocols to move funds at unprecedented speed and scale—automating obfuscation and fragmenting visibility across networks.

These tactics are increasingly observed in high-priority threat areas, including sanctions evasion, geopolitical interference, darknet financing, and complex financial fraud—challenging conventional methods of detection and disruption.

Tracker is Merkle Science’s blockchain investigation platform, purpose-built for law enforcement, intelligence, and national security teams. It delivers automated tracing, cross-chain continuity, and transparent attribution to support fast, defensible, and coordinated investigative action. This brochure provides an operational overview of Tracker’s core capabilities designed to meet the investigative demands of speed, accuracy, and forensic-grade attribution. Every feature in Tracker is engineered for real-world casework— enabling agencies to follow the money, no matter where it moves.

Tracker is trusted by public sector agencies across mission areas including:

Counterterrorism and
terrorist financing

Darknet market
disruption

Cross-border laundering
investigations

Sanctions exposure
monitoring

Human trafficking and
exploitation finance

State-sponsored and
organized crypto crime

The Need for Advanced Crypto Investigations

Crypto-related financial crimes are increasingly sophisticated, with illicit actors leveraging smart contracts, bridges, and swaps to launder funds at unprecedented speeds. Traditional investigation tools struggle with delays, incomplete data, and limited attribution capabilities. Tracker provides automated tracing, cross-chain forensics, and real-time risk assessment to trace illicit funds in real time, expose laundering tactics, and build airtight cases—as criminals cash out.

This brochure outlines the core capabilities that make Tracker operationally distinct. It is structured around key investigative workflows, each built to support law enforcement teams across real-world case scenarios:

- Automated Tracing
- Attribution Transparency
- Cross-Chain Forensics
- Collaboration & Reporting
- Smart Contract Analytics

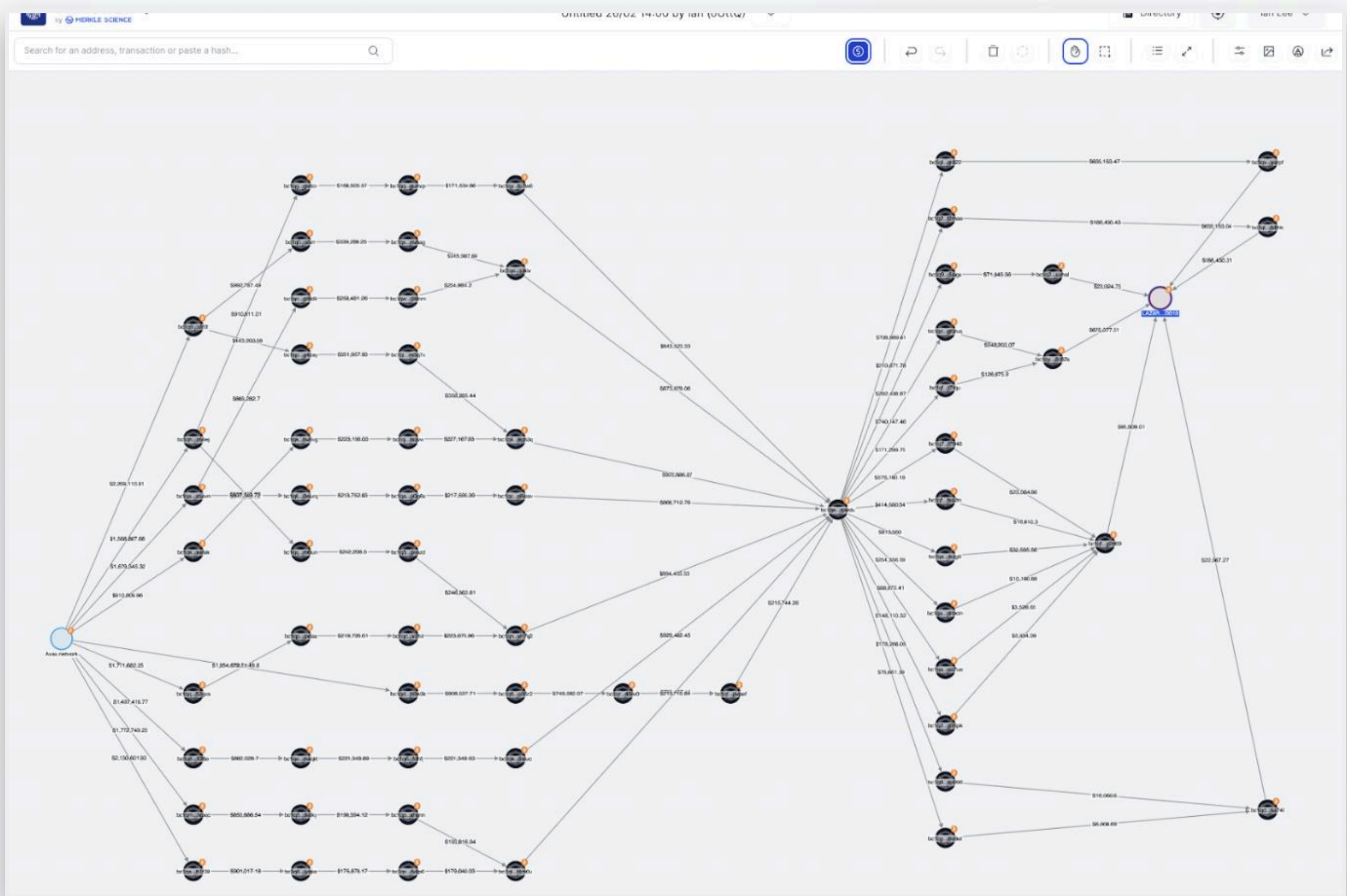
Each section demonstrates how Tracker enables faster case development, actionable intelligence, and outputs that meet legal and operational standards.

1. Core Investigation Features

Auto-Tracing - Map Every Fund Movement—10x Faster

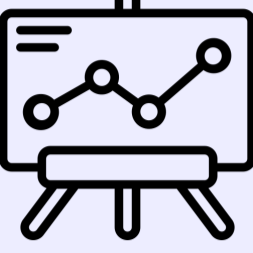
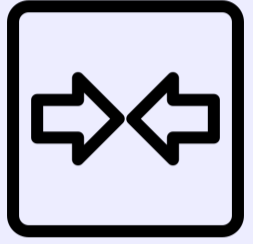


Illicit assets rarely move in a straight line. Transactions fragment across chains and services, making it difficult to identify all exit points or time-sensitive exposure. Without full-path tracing, critical leads can go undetected—and enforcement delayed.

Investigators need automated tracing that matches the speed and complexity of modern laundering tactics. Tracker’s Auto-Tracing maps all possible fund flows, ensuring no key movement is missed and every investigative angle is explored.



Why This Matters

In many cases, investigators trace funds to a known exchange or high-risk service—only to realize later that parallel transactions exited through lesser-known paths: a secondary bridge, a mule wallet, or a wrapped asset on another chain. Without visibility into all potential fund flows, subpoenas may be delayed, seizures incomplete, and criminal networks left partially exposed. AutoTrace helps uncover these secondary paths instantly, helping agencies act before funds are lost or suspects re-engage.

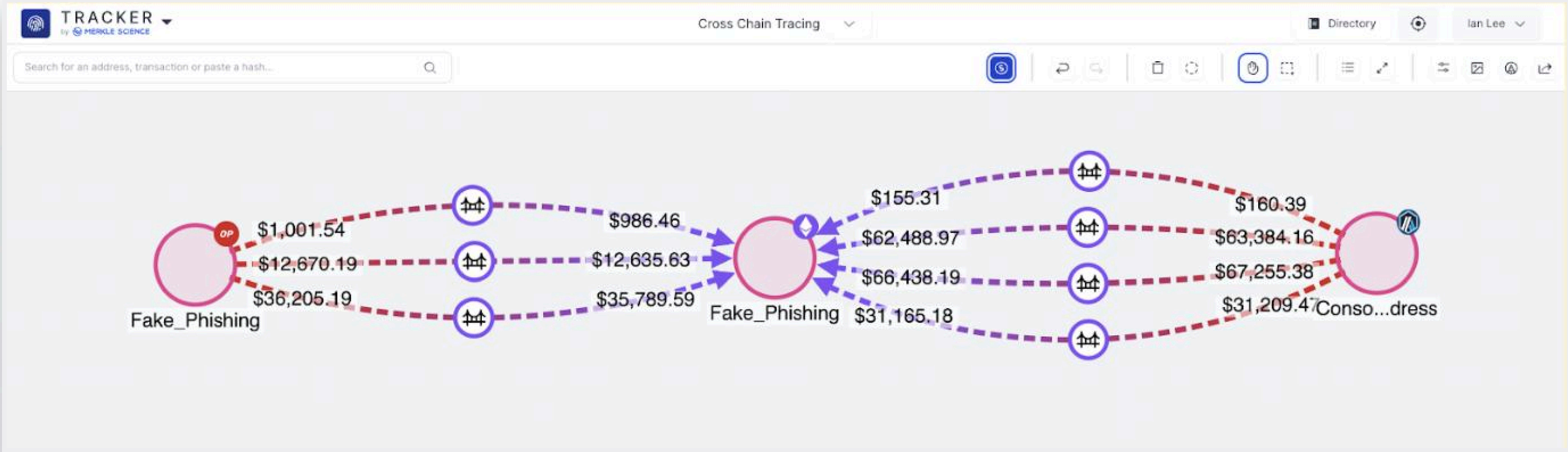
Key Capability	Benefit
 Full Exposure Pathway	Automatically map all possible fund flow pathways—ensuring no transaction is overlooked. Unlike other tools that only show the shortest route or largest transaction, Tracker traces every possible movement of funds, ensuring that all leads are captured.
 Entry & Exit Point Detection	Track how illicit funds move through on-ramps, off-ramps, and high-risk entities, uncovering key touchpoints in the laundering process. Detect when funds enter exchanges and VASPs, so you can quickly pinpoint where to request KYC records and accelerate case resolution.
 High-Risk Entity Exposure Identification	Instantly flag addresses with ties to sanctioned entities, darknet markets, and illicit actors.
 Custody Change Detection	Track how assets change hands to uncover hidden ownership structures.


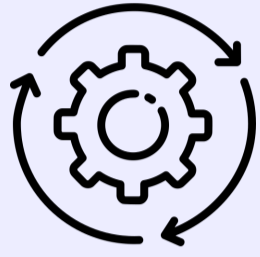
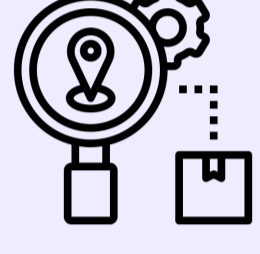
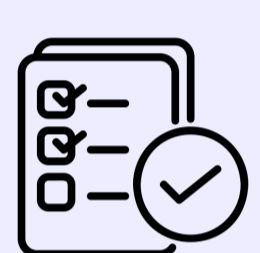
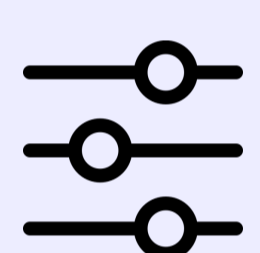

Auto-Connect: Intelligent Link Analysis

Tracker automatically identifies transactional links between addresses, removing the reliance on manual analysis. When a new address is added, Tracker instantly detects direct interactions, maps relationships, and compiles transaction history, enabling investigators to quickly visualize fund flows and associated counterparties

Cross-Chain Investigations

Crypto criminals frequently use rapid cross-chain transactions and "noise bombing"—intentionally fragmenting the investigative trail and overwhelming traditional tracing tools. Tracker’s automated cross-chain analysis quickly cuts through this deliberate obfuscation, instantly mapping fund movements across multiple chains and bridges, giving investigators clear visibility into real transaction patterns.

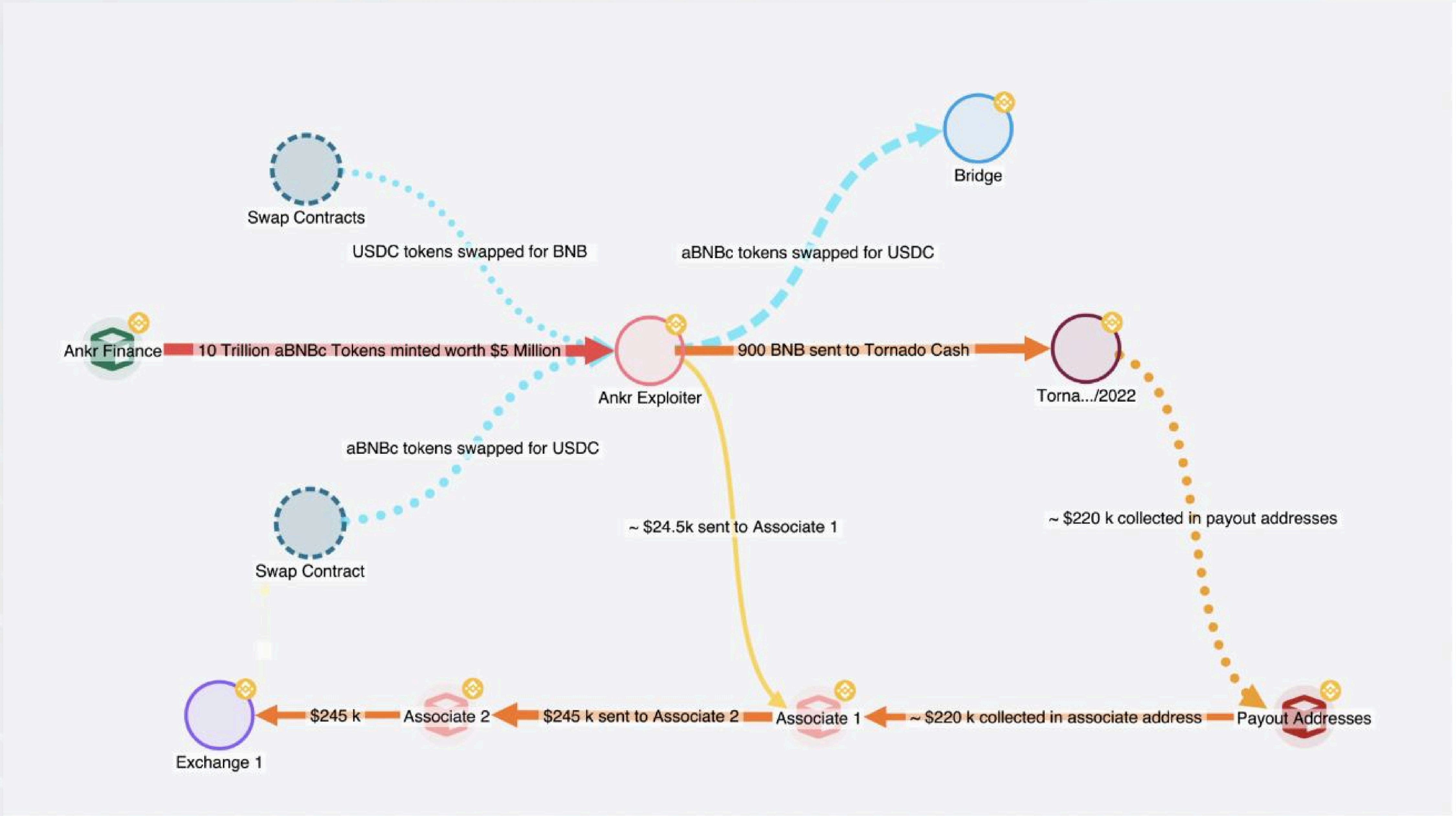


Key Capability	Benefit
 Real-Time Decoding Across 250+ Blockchains	Instant access to bridged transactions ensures investigators have the most current data accelerating response times and eliminating data sync delays.
 Automated Asset Identification	Immediately identifies and labels bridged assets, wrapped tokens, and liquidity movements.
 Automated Tracing	Automatically traces funds across 60+ bridges and 2,000+ smart contracts .
 Instant Validation	Direct bridge explorer links enable quick transaction verification, ensuring investigative accuracy and facilitating parallel reconstruction.
 Advanced Filtering	Quickly narrow down searches by transaction type, amount, protocol, and counterparty, cutting through noise to identify high-risk transactions faster.
 Cross-Chain Bridges Data Directory	Offers a clear overview of supported bridges, transaction parsing statuses, and validation reports, enhancing transparency in cross-chain analysis.

Why This Matters

Most tools rely on delayed indexers or incomplete bridge coverage, forcing investigators to wait hours—or manually stitch flows—before they can trace funds across chains. Tracker eliminates this lag with live decoding, allowing teams to reconstruct cross-chain flows immediately and act while funds are still in motion.

For evidentiary needs, instant validation via bridge explorers allows investigators to confirm transaction paths without leaving the platform—removing the need to replicate traces across OSINT tools and reducing time to subpoena or seizure.



Watchlist: Real-Time Monitoring & Alerts

Tracker provides proactive monitoring and real-time alerts across all supported blockchains, keeping investigators ahead of illicit activity. Alerts can be set on high-risk addresses, triggering instant notifications when stolen funds move, dormant wallets reactivate, or suspects attempt cash-outs—ensuring investigators can act before funds disappear.

- Customizable alerts**
Configure notifications based on transaction type, direction, and amount, prioritizing critical events.
- Collaborative tracking**
Share alerts across teams to coordinate responses and accelerate investigations.

WATCH THE ADDRESS

Only Incoming Funds

Only Outgoing Funds

Both

MINIMUM DOLLAR VALUE

\$ 0

MAXIMUM DOLLAR VALUE

\$ Max

TRANSFER TYPE

All

Token Transfer

External Transaction

Internal Transaction

While this feature does not use explicit “risk scores,” users can define threshold-based rules that function as custom risk logic—prioritizing alerts tied to high-value flows, sanctioned tags, or reactivated addresses

Attribution & Clustering – Transparent, Defensible, and Field-Tested

Attribution is only as useful as it is explainable. Tracker combines validated heuristics and structured behavioral patterns to form clusters investigators can rely on—both in active casework and evidentiary settings.

Each address grouping is generated using rule-based logic, validated through structured review, and visible to the user within the platform. Whether identifying darknet vendors, exchange service clusters, or bridge-funded laundering routes, Tracker provides attribution that is transparent, repeatable, and built for audit.

Core Attribution Features	What It Does
Deterministic Heuristics	Uses inputs like common ownership (Bitcoin), contract reuse (Ethereum), and gas funders to group wallets under clear control patterns.
Behavioral Attribution	Detects laundering typologies like peel chains, nested flows, or repeated counterparty exposure.
Cross-Chain Propagation	Automatically links known clusters across EVM chains using deployer tagging and token distribution paths.
Attribution Transparency	Every link is backed by explainable logic and shown within the platform—no opaque tags or hidden inferences.
Investigator Feedback Loop	Field teams can challenge, confirm, or extend clusters, triggering internal review and dataset updates.



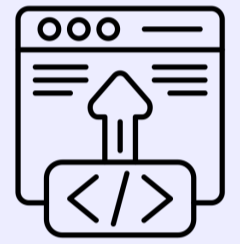
2. Advanced Investigation Features

Built for investigators handling complex DeFi laundering schemes, Tracker provides greater visibility into smart contract activity, transaction details, and hidden on-chain connections.

Smart Contract Analytics

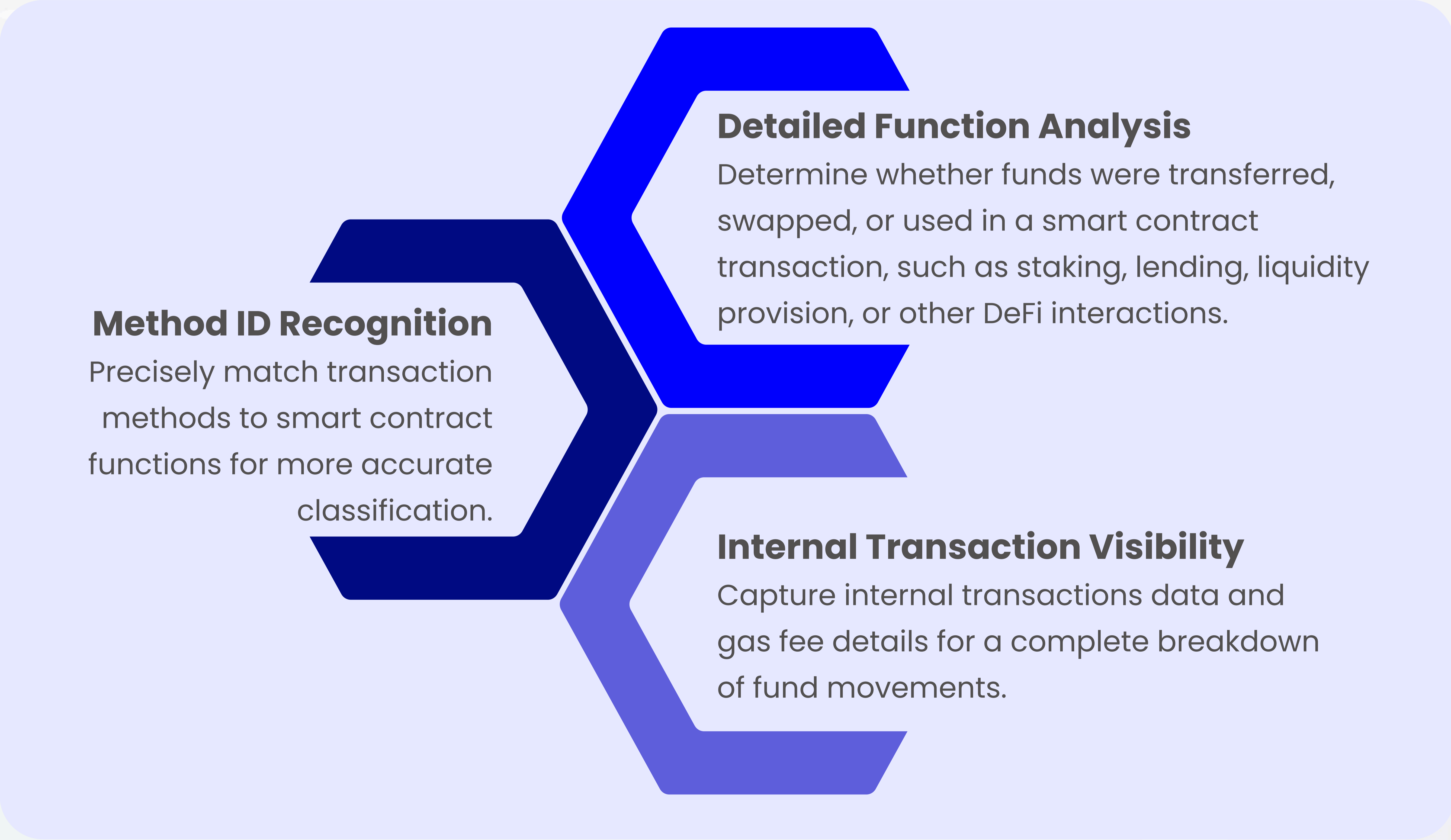
Illicit actors increasingly use custom contracts, clones, and proxy deployments to obscure laundering flows. Tracker helps investigators go beyond token-level tracing to understand what a contract does, who deployed it, and how it links to other activity

Tracker enables detailed smart contract analysis, helping investigators identify contract creators, funding sources, and high-risk contract interactions — exposing patterns across forks, exploit kits, and scam infrastructure. This allows agencies to link incidents, detect early-stage deployments, and identify repeated laundering tactics.

Key Capability	Benefit
 Contract Creator Identification	Identify who funded a smart contract deployment and trace connections to known actors, past deployments, or potential illicit activity.
 Code Similarity Analysis	View all contracts created by the same entity, identifying broader patterns of activity.
 Deployment History	Detect smart contracts with high code similarity, uncovering potential clone contracts, unauthorized forks, or coordinated on-chain activity.

Expanded Transaction Metadata

Tracker provides detailed visibility into each transaction, helping investigators quickly determine transaction types and accurately analyze fund movements.



Why This Matters

Traditional tools often stop at simply labeling tokens or exchanges, offering little insight into who deployed a contract or its linkage to previous incidents. In contrast, Tracker automatically attributes the contract itself, revealing funding trails, creator wallets, and behavioral links across chains. This enables investigators to flag repeat deployers, detect early-stage scams, and take action before fraud scales—without needing to decode complex contract logic.

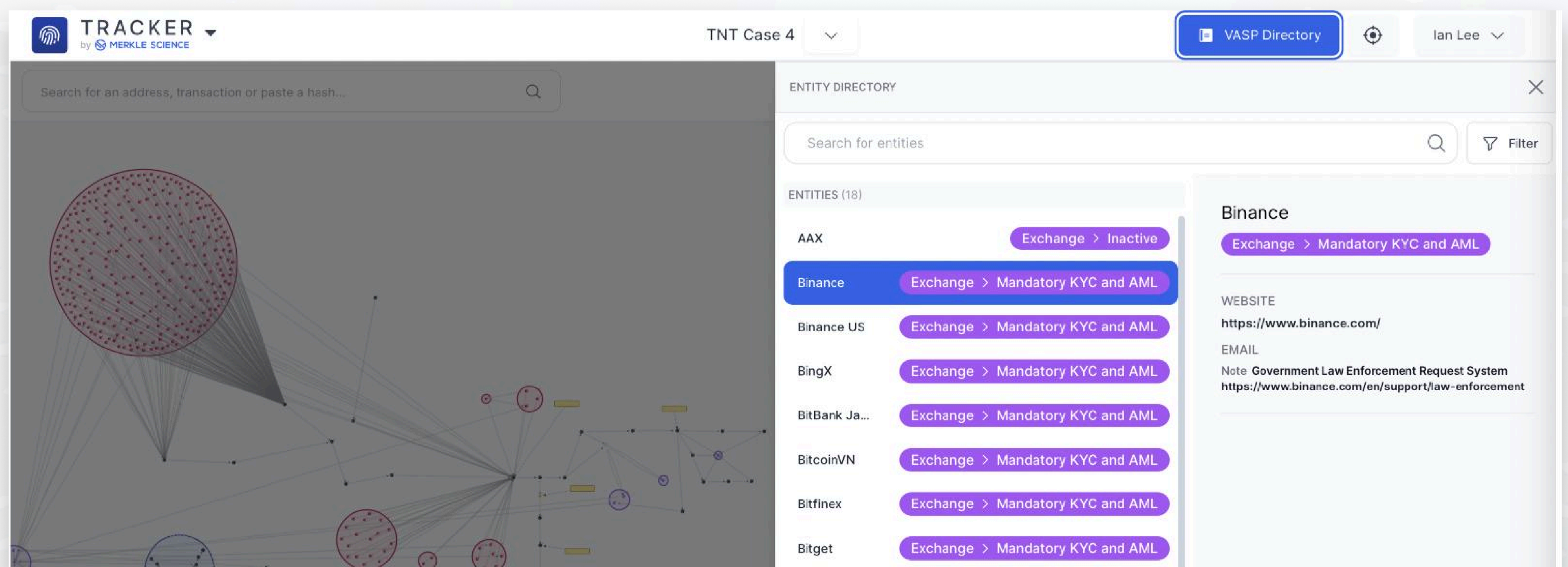
3. Collaboration & Intelligence Sharing

Investigations don't happen in silos. Tracker allows law enforcement, intelligence, and regulatory teams to share active case boards, timelines, and findings across units—without needing additional licenses or technical overhead.

Investigators can export trace evidence, share encrypted links with prosecutors or task forces, and generate reports that stand up in court

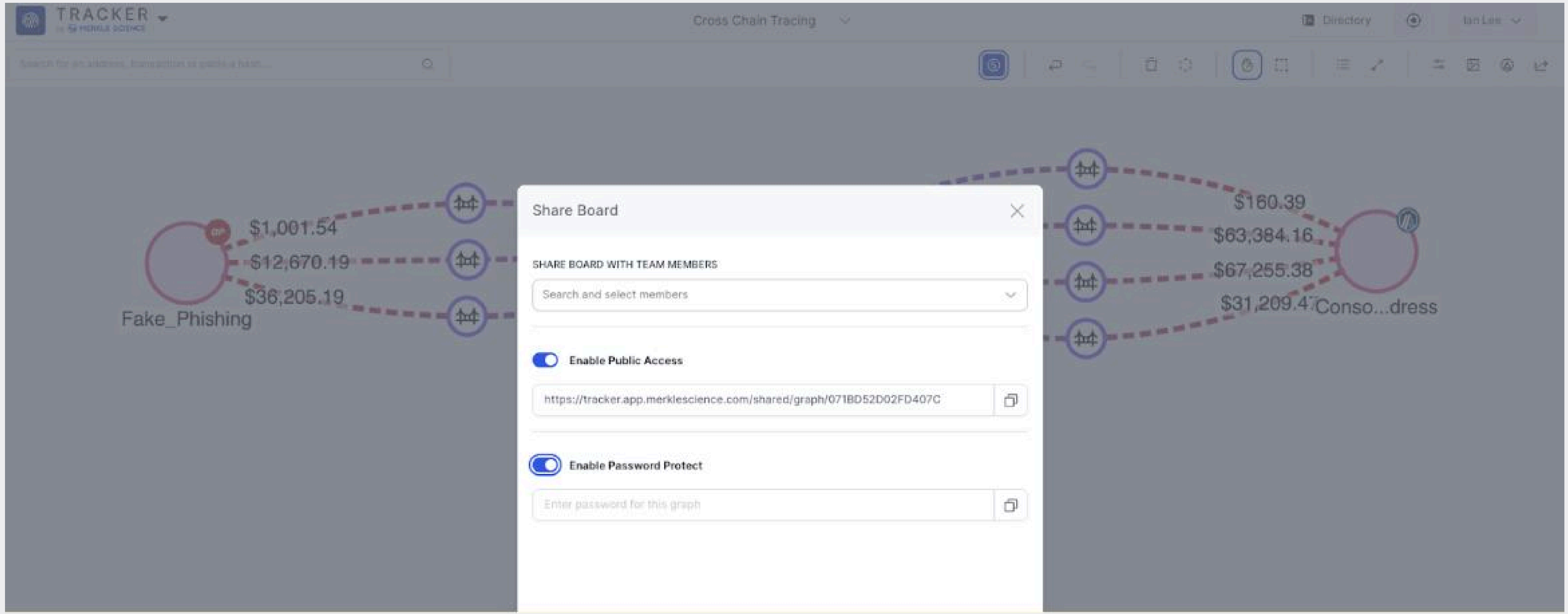
VASP Directory: Exchange & Compliance Requests

Tracker provides instant access to exchange contacts through its VASP Directory, allowing you to quickly request fund freezes, obtain KYC records, and track illicit transactions back to real-world identities. This streamlines investigator outreach, ensuring you can act fast before criminals cash out.



Investigation Sharing

Tracker enables investigators to securely share case boards with internal teams and external partners—including those without a Merkle Science license. Boards are shared via protected URLs with optional password protection, facilitating efficient collaboration while maintaining investigative integrity and data security.



4. Court-Ready Attribution: Build Cases That Stand Up

Many blockchain analytics tools fail to provide clear, legally defensible evidence. Tracker ensures that every piece of data meets courtroom standards. Tracker ensures investigations meet forensic and legal standards, providing verifiable attribution and court-admissible reports to support prosecution and compliance efforts. Every attributed address undergoes Merkle Science’s validation process, with source data, images, and metadata stored as part of the evidence trail for full transparency.

Service	Description
Attribution Source Reports	Detailed breakdowns of transaction attribution, dusting exercise, clustering methods, and validation processes.
Enhanced Due Diligence Reports	Generate comprehensive investigation reports where specialists reconstruct cases end-to-end for complex inquiries.

Advanced Demixing: Tracker supports on-demand, heuristic-based tracing for mixer activity (e.g., Tornado Cash), using deposit–withdrawal correlation and timing analysis to identify likely linkages between sender and recipient.

IP Intelligence and Geolocation Insights: When needed, geolocation enrichment reveals regional behavior clusters and infrastructure hotspots—powerful tools for attribution and escalation.

Requesting De-mixing Services

1. User submits a support ticket within Tracker with the Subject “Demixing Request” with the following information:
 - a. **Address**
 - b. **Transaction Hash**
 - c. **Mixer Name (if known)**
2. Merkle Science intelligence department will review the request and generate a report in approximately 3–30 days.
3. User may request for a call with Merkle Science intelligence team to review findings.

TRACKER
by MERKLE SCIENCE

Untitled 20-03 22:22 (MixXM) by IL

Search for an address, transaction, entity or paste a hash...

Leave us a message

Product Support

Email address
ian@merklescience.com

Subject
Demixing Request

Description
Please enter the details of your request. A member of our support staff will respond as soon as possible.
Can you assist with demixing transaction 3d7a8858632042e2474f0fa52684681a5b8117f00d5aca23b74366695424c011 from bc1qce560x65wghdpfv5z5jydpd67awu2wmyenwje6 into Wasabi

Send

Requesting IP Data

1. User submits a support ticket within Tracker with the Subject “IP Data Request” with the following information:
 - a. **Address**
 - b. **Blockchain**
2. Merkle Science intelligence department will review the request and generate a report in approximately 3–7 days.
3. User may request for a call with Merkle Science intelligence team to review findings.

TRACKER
by MERKLE SCIENCE

Untitled 20-03 17:06 (p6eai) by IL

Search for an address, transaction, entity or paste a hash...

Leave us a message

Product Support

Email address
ian@merklescience.com

Subject
IP Data Request

Description
Please enter the details of your request. A member of our support staff will respond as soon as possible.
Please provide IP data associated with Bitcoin address bc1qaq28t6ct8603m6v57izujf7utg6nyzwv3xtuwn

Send

Ready to Investigate Without Blind Spots?

Tracker helps investigative teams trace faster, attribute with confidence, and act before funds disappear. For demo access, case support, or technical documentation, contact the Merkle Science investigations team:

Learn more or request a demo today.

www.merklescience.com

