neuTracker

Bitcoin Tracking for Forensic Investigators

A private, self-hosted monitoring platform that watches addresses, public keys and transaction patterns on your behalf — and delivers classified, case-ready alerts the moment the chain moves.

In this brief

- Why tracking — not just searching — is what cases actually need
- The four things neuTracker can track, and why public-key tracking is the game-changer
- The thirteen event types the classifier produces, and how alert levels escalate
- Back Trace: reconstructing history the moment a new target lands on your desk
- Where neuTracker lands differently from Chainalysis, TRM, Elliptic and Crystal

Searching is not enough

Every forensic Bitcoin product on the market can search the chain after the fact. That works when you already know where to look. It stops working the moment your subject rotates to a new address, a new wallet format, or an address that has never appeared on-chain before. By the time a human thinks to re-query, the trail is cold.

Tracking flips the model. Instead of asking "show me what this address has done," you tell neuTracker "tell me the moment this address — or anything derived from it — does anything." The server classifies each new transaction against every watched target as it is indexed and pushes a priority-ranked alert to the analysts who need to see it.

> *Chain analytics catches what already happened. neuTracker catches what is happening — and tells you what it means in the same notification.*

Built for the way investigators work

neuTracker's Tracking subsystem is opinionated about four things a real case needs and competing products routinely get wrong:

1. **Confidential queries.** Every lookup stays on your hardware. Nothing tells a third party which address your grand jury cares about. SaaS chain-analytics vendors log every query — neuTracker does not have that risk surface because there is no SaaS.
2. **Classification, not a firehose.** Alerts arrive pre-labelled (Received from OFAC, Dormancy Wake, Consolidation, Sent to Named Entity). Investigators do not triage row-by-row in a spreadsheet.
3. **Public-key depth.** When a single target spends, neuTracker recovers the public key and automatically cascades the watch to every sibling address that shares it — including addresses that have never broadcast a transaction yet.
4. **Retroactive reconstruction.** Back Trace regenerates the full historical event stream for a newly flagged target, so a subject added today comes with an immediate case file, not an empty one.

What you can track

The Tracking Page watches four distinct classes of blockchain artefact. Each has a different operational role in an investigation.

Address — A single Bitcoin destination, in any format: legacy P2PKH, multisig / wrapped SegWit P2SH, native SegWit Bech32, or Taproot Bech32m. The workhorse tracker. Every inbound or outbound UTXO that touches the address produces a classified event.

Public Key — A raw EC public key, independent of address format. This is where neuTracker goes beyond the competition: a single private key can derive compressed, uncompressed, SegWit-wrapped and Taproot addresses that — to most tools — look like four unrelated targets. neuTracker collapses them into one watch. Adding a new subject address automatically pulls in every sibling that shares the key, even siblings that have never appeared on-chain.

Transaction — A specific transaction hash, pinned as a case artefact. Subscribers attach per-group notes and tags and receive a single confirmation event when the transaction lands in a block. Useful for tying evidence to warrants and filings.

Block — A specific block height, used as a case bookmark. Typical uses: fixing the moment of a seizure, pinning a fork activation, time-boxing a range of tracked activity.

Known vs. Tracked — two roles, one engine

Any tracked object can also be flagged “Known.” Known objects are the canonical list of entities your team has positively identified: an exchange's hot wallet, a seized mixer address, an OFAC-sanctioned address, a co-operating custodian.

The classifier automatically escalates any interaction between a tracked subject and a Known entity to the highest alert level — Critical — without requiring a separate monitoring rule. Import OFAC's SDN list once and every tracked customer address is screened against it on every transaction forever.

Deep search, not just chain search

When a tracked address appears in a new transaction, neuTracker's classifier asks a prioritised series of questions about the counterparty before it writes a single event row. This is the “deep search” layer that differentiates neuTracker from explorers and SaaS products that just return a list of hashes.

1. Is the counterparty in the Known list? Seizure wallets, OFAC / SDN entries, identified exchanges, named criminal infrastructure. If yes, the event is emitted as SentToKnown / ReceivedFromKnown at Critical severity.

2. Does the counterparty share a public key with the subject? neuTracker consults its own pubkey↔address map — populated by watching spends across the entire chain — to decide whether the counterparty is really just another wallet belonging to the same private key. If yes, the event is SentToSelf / ReceivedFromSelf. This is the check competitors miss.

3. Has the counterparty been named by my Tracking Group? Analyst-curated names (“Binance Hot 3,” “Suspect-A Laundering Wallet”) are per-group and private. A match elevates the event to High severity and carries the human-readable name into the alert payload so the oncall officer immediately understands what happened.

4. Otherwise. The event is a vanilla Sent (Medium) or Received (Low). Still captured, still visible, still forms part of the wallet graph — but it does not page a human out of bed.

Pattern detection, not just point events

On top of per-counterparty classification, the server inspects the overall shape of each transaction the subject participates in:

Consolidation — Many inputs collapsing into few outputs. The signature of a sweep, cold-storage transfer, or exchange omnibus-wallet roll-up. Often the earliest warning that a subject is preparing to move or exit.

Distribution — Few inputs fanning out to many outputs. The signature of payroll, airdrops, mixer post-processing, or a ransomware operator splitting proceeds across cash-out rails.

Activity-Time Threshold — The subject has just moved after a group-configurable dormancy window (30 days, one year, five years, whatever matches the case). The single most valuable alert in cases involving long-dormant wallets: heir claims, sanctions evasion via old miner coin, ransomware key recovery, and estate disputes.

Public-Key Identified — The moment a subject's public key is first recovered from a spend, the watch automatically extends to every sibling address that shares the key. Names and tags propagate across the entire cluster in the same event.

The thirteen event types at a glance

Every alert neuTracker raises falls into exactly one of these categories. The colour swatch below each severity matches the Alert Level badge colour used in the Tracking Page UI.

	CRITICAL	Sent to Known • Received from Known
	HIGH	Sent to Named • Received from Named • Activity-Time Threshold
	MEDIUM	Sent (unknown counterparty) • PubKey Identified • Consolidation • Distribution
	LOW	Received (unknown counterparty) • Sent to Self • Received from Self
	INFO	Message (analyst broadcast, not chain-driven)

Per-group alert thresholds. Each Tracking Group assigns a minimum severity to each of its registered devices. Field laptops can page on Critical only; the case officer's workstation can page on High; the analyst console sees the full firehose. The server honours the threshold when it dispatches — nobody is paged off-shift for a routine change output.

Real-time and historical in one pipeline

Live alerts: As neuTracker indexes each new block, every transaction is scored against the full watch-list. A matched tracked object produces an AlertMessage that is pushed over WebSocket to connected clients and dispatched as e-mail / MMS to every Group device subscribed above the event's severity. Typical end-to-end latency from block arrival to a detective's phone: seconds.

Back Trace: When a new target lands on your desk mid-case, the events table for that target is empty for everything that happened before you flagged it. Back Trace walks the subject's full historical transaction list within an analyst-chosen date window and synthesises events as if the tracker had been running the whole time. The option to replay those events as live notifications makes case hand-off to a responding team automatic: Back Trace with Notify on, and the incoming team receives the complete timeline in the same channel as the live stream.

Case patterns

Representative workflows that neuTracker's Tracking subsystem was designed to serve. All are drawn from real public-record investigations.

OFAC / sanctions screening — Import the Treasury SDN list's Bitcoin addresses once and mark each Known. Every tracked customer-deposit address thereafter screens against the full list on every transaction. Any match raises a Critical SentToKnown / ReceivedFromKnown event with the sanctioned counterparty, timestamp, amount and transaction hash captured in the alert payload — ready for SAR filing.

Ransomware case build-up — Flag the initial ransom-receiving address. As the operator sweeps through intermediate wallets, Consolidation events fire; as proceeds fan to mixer deposits, Distribution events fire; as they reach named cash-out venues, High-severity SentToNamed events carry the human narrative directly into the evidentiary log.

Dormant-whale awakening — Tag long-dormant miner coin with a multi-year Activity-Time Threshold. When the address finally moves, a single High alert fires — often hours before the movement surfaces on social media. The spend reveals the public key, triggering a PubKey Identified cascade that brings every sibling address under watch automatically.

Darknet market / mixer takedown — On seizure day, flag the market's primary withdrawal address and mark it Known. Every existing tracked subject in the database is automatically screened against it going forward — any residual interaction produces a Critical event, without a single new rule.

Estate / missing-persons recovery — Flag the decedent's or missing party's last-known address. Any spend is, by definition, a Sent event — immediately contradicting a presumption that the key was lost. The counterparty address and recovered public key are captured automatically for subpoena or interview.

Bankruptcy / receivership claw-back — Seed the tracker with every address referenced in the estate's filings. As newly discovered addresses come in, Back Trace rebuilds the full historical flow of victim funds through the cluster. Named-counterparty labels (“Victim 0042 Deposit”) feed downstream restitution calculations directly out of the trackedevents table.

Internal tumbler / self-shuffle detection — A subject running in-house mixing shows up as a sustained stream of SentToSelf and ReceivedFromSelf events once neuTracker has recovered their public key. The ratio of Self-classified to anonymously-classified activity quantifies how much of the subject's volume is internal noise versus genuine external flow.

How neuTracker differs from the incumbents

Your queries never leave your network. Chainalysis Reactor, TRM Labs, Elliptic Investigator and Crystal Expert are SaaS platforms. Every address you investigate is a query against a vendor's infrastructure — with the logging, retention, subpoena and insider-risk implications that implies. neuTracker runs on your hardware, inside your network, under your change-control. The vendor sees nothing because the vendor is not in the path.

Public-key cascade, not heuristic clustering. Competing products cluster by behavioural heuristics: co-spending, common input ownership, timing correlation. Heuristics are probabilistic and fail on sophisticated targets that specifically avoid co-spending. neuTracker's sibling-address detection is cryptographic — two addresses are linked iff they derive from the same public key. No probability, no false clusters, no expert testimony about confidence intervals.

Active alerts, not attribution reports. SaaS products answer "who owns this address?" after the fact. neuTracker answers "what just happened to the addresses you care about?" within seconds of block confirmation, classified, ranked and delivered to the device your investigator is carrying.

Per-group case context travels with the alert. Analyst-curated names, tags and notes are attached to tracked objects and carried inside the alert payload. The officer receiving the page does not need to pivot to a second product to find out why the address matters — the context is in the notification.

One-time capital expense, not per-seat SaaS. neuTracker is licensed per server, not per seat. Add analysts without adding invoices. Scale the number of tracked objects without triggering a tier-upgrade conversation with a salesperson.

> *When the chain moves, the question is not "can I look it up?" The question is "did I hear about it in time?" That is the question neuTracker is built to answer.*

Take the next step

neuTracker is available for on-premise deployment with dedicated professional-services support for agency evaluation, threshold tuning, and integration with existing case-management systems.

We offer evaluation licences and structured proof-of-value engagements for qualifying law-enforcement, regulatory and compliance teams. Contact us through the neuTracker website to schedule a briefing, request access to a live demonstration server, or arrange a no-cost evaluation on a case of your choosing.