PROVENANCE TRANSPARENCY · A PROPOSAL · OCTOBER 2026

Crypto safety data without a paywall

Warnings about stolen or scam-linked crypto are mostly locked inside paid products. Vendor labels reportedly cost $26k to $295k a year, aimed at exchange compliance teams. The free alternatives are throttled (the largest free report site caps standard API keys at 10 calls a month) or have gone dormant. In a recent case, a $1M proof-of-funds theft was one of about 46 incidents, worth about $16M, by a single ring. Almost none of its wallets carried a public warning until the victim's team filed them by hand.

The idea is to separate facts from judgments, as Certificate Transparency and CVE do. We propose a free, append-only public log of evidenced claims. An entry says that funds from a given transaction are proceeds of a given incident, with signed evidence hashes, an issuer and a confidence level. It never says "this person is a criminal." Corrections are new entries (disputed, withdrawn, superseded), not deletions. Wallets and individuals read it free through a privacy-preserving hash-prefix lookup. Each wallet, exchange or vendor applies its own policy.

Funding does not depend on selling labels. Victims' counsel pay filing fees to place entries, because logged notice helps establish that a later recipient knew. Exchanges get free bulk access in return for contributing their own confirmed deposit-address data. Issuers can attach an opt-in recovery pledge, which needs legal structuring. Public-goods grants cover the rest. Commercial vendors sell scores, clustering and service levels on top.

The legal defence is the design. The log publishes evidenced facts about transactions, not accusations against named people. Independent operators and scoped, accredited issuers carry the load. Every entry has a free dispute path with a fixed window and an evidence standard. Address-privacy law can be handled through an erasure process for people who prove innocence.

We are asking for two independent operators (a university or security collective), a first exchange willing to reciprocate, and public-goods funding for a 90-day bootstrap. Infinihash will build the reference implementation and act as first issuer. It will not own the log.

Working title; alternatives: Open Ledger of Notice, The Safety Commons. Figures are from the accompanying research notes; vendor prices are third-party estimates. The recovery pledge needs legal structuring before use.