

UNYKORN IMPACT & INNOVATION REPORT • EDITION 2026 • COMPANION

Blockchain *Fraud*

Integrity and recovery without the second scam: a free check, flat-fee cases, sealed evidence, and monitoring that keeps running.

UnyKorn LLC September 2026 Edition 1.1

Why it exists

People who lose money to a crypto scam are immediately targeted again, this time by "recovery agents" who ask for a fee up front or a share of whatever is recovered, and deliver a PDF of guesses. The market lacked a desk that would tell someone plainly whether their evidence was sufficient, do bounded work for a fixed price, and refuse to promise a result.

blockchainfraud.org was rebuilt in September 2026 after its earlier deployment was found deleted from the account. The rebuild started from the money loop and worked outward: a free check first, so nobody pays to learn they have no case.

No recovery is promised. No percentage is charged. If the evidence is thin, the check says so before anyone pays.

Global context

Fraud is now measured in the tens of billions a year by the FBI alone, and misinformation is the top short-term global risk in the WEF survey. A desk that refuses to promise recovery and charges a flat fee is a small answer to a large number, and this report does not pretend otherwise.

EXTERNAL

FBI Internet Crime Complaint Center · 2024 Internet Crime Report

Record losses; cryptocurrency fraud figures; age-group data.

Ca new record for losses reported to IC3, totaling a staggering \$16.6 billion
149,686 complaints; \$9.3 billion in losses; 66% increase in loss; largest age group to report is 60+

https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf · retrieved 2026-09-09

EXTERNAL

World Economic Forum · Global Risks Report 2025 (20th edition, 15 January 2025)

Top short-term risks; survey of over 900 experts.

Misinformation and disinformation remain top short-term risks for the second consecutive year

<https://www.weforum.org/press/2025/01/global-risks-report-2025-conflict-environment-and-disinformation-top-threats/> · retrieved 2026-09-09

What we built

A single Worker serves the analyzer app and its API; a database holds cases, registrations, evidence chains and receipts; a separate watchtower Worker runs the monitoring API and the Telegram bot on the same engine as the site.

FREE

Scam check in the browser

Patterns scored client-side with ranked signals and a downloadable PDF; nothing is uploaded.

INTAKE

A real back end

Form to database row to case ID on screen, with an owner email from cases@; honeypot and validation on the live form.

ASSESSMENT

Bounded trace on every intake

Any intake with a wallet gets a genesis and flow trace; the assessment renders with the matching pay link.

EVIDENCE

Vault

Browser-side encryption with envelope keys, digest-addressed storage, a chain entry per file, handler-side opening.

MONITORING

Watchtower API

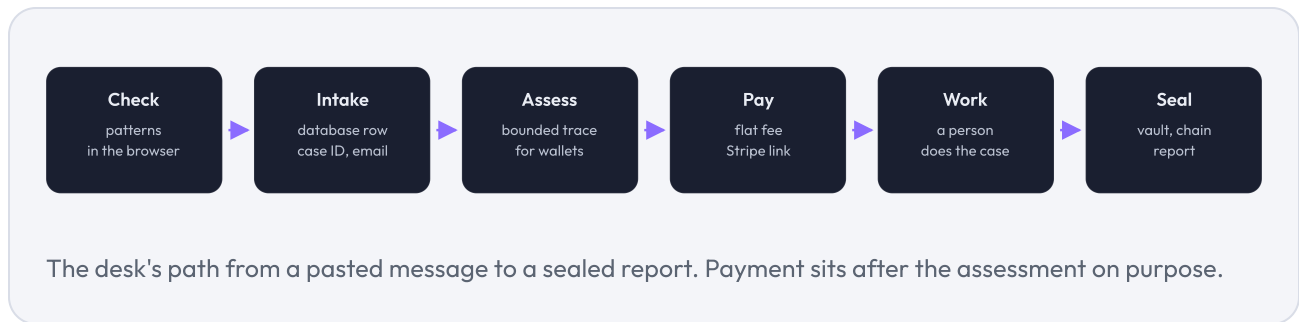
Cases, alerts, evidence-chain verification, a sweep, reports, a registry and the sanctions list.

REACH

Telegram bot and narrators

A bot with the same engine; three named narrators pre-rendered on every fixed page.

How it works



The check never leaves the browser. Only when someone opens a case does data move, and then to a database the founder controls, with an evidence chain whose digests can be recomputed by anyone holding the files.

What is real today

Every row is a ledger row: the label, the evidence method and the command are in the published ledger.

CAPABILITY	EVIDENCE	STATE
blockchainfraud.org served-site checks	209 checks pass, 0 fail, against the live site.	MEASURED
Free scam check, in-browser	43 patterns evaluated client-side with ranked signals and a PDF; nothing uploaded.	CAPABILITY
Sanctions screen	478 sanctioned addresses imported into the watchtower registry.	MEASURED
Blockchain Fraud flat-fee products	Six live Stripe products: trace \$750; full investigation \$1,750 retainer + \$1,750 balance; security retainer \$2,500/month; Case Watch \$249/month; Cluster Watch \$1,250/month.	MEASURED
x402 v2 gateway (USDC on Base, eip155:8453)	Five priced endpoints answer a correct 402 challenge with the treasury as payee; mainnet settlement is not configured (no Base facilitator key), so paid retries are answered with the challenge and nothing is charged.	GATED
Percentage-of-recovery fees, commissions, affiliate payouts	None anywhere on UnyKorn LLC surfaces; a hard rule. (A referral table with a "commission" column exists in platform.unykorn.org's code; that surface is flagged for the estate sweep, not cited as UnyKorn LLC pricing.)	MEASURED

Trust and safeguards

The copy is scanned for the phrases we refuse to use. The site says in plain words that no recovery is promised and that a case may end with "insufficient evidence". Credentials for the bot, payments and email are worker secrets.

Economics

Flat fees, published, chosen so that a person with a small loss and a company with a large exposure both know the price before they start.

PRODUCT	PRICE	STATE
Trace	\$750	MEASURED
Full investigation (retainer + balance)	\$3,500	MEASURED
Security retainer	\$2,500 / month	MEASURED
Case Watch	\$249 / month	MEASURED
Cluster Watch	\$1,250 / month	MEASURED
Address screen for agents (x402)	per call in USDC, see the manifest	GATED

Next phase

Workers Paid to remove the CPU ceiling; object storage for sealed evidence; a paid block-explorer plan to add more chains to automated tracing; then the first quarter of published case counts in Edition 2027.

Sources. ledger rows INS-BF-*, CH-X402, INS-COMP-RULE; docs/LAUNCH-STATUS-2026-09-09.md; docs/REVENUE-MAP.md

UnyKorn LLC is a technology and administration service provider. It is not a bank, broker-dealer, exchange, custodian, trustee, transfer agent, appraiser, auditor, investment adviser, money transmitter, or issuer. Nothing in this report is an offer, a solicitation, legal advice, or a promise of any outcome. Client engagements conducted under separate operating entities are not included.

UnyKorn LLC, a Wyoming limited liability company formed July 1, 2026 (Wyoming filing 2026-002019968). Edition 1.1, September 2026. Every figure in this report is bound to a row in the evidence ledger; the whole ledger is published at /report/ledger.json. Anything that could not be resolved to a re-runnable command, an API response, an on-chain read or a hashed document with a date is labelled honestly or omitted. Corrections: hello@blockchainfraud.org.

MEASURED produced by a command, API call or on-chain read recorded in the ledger row and re-runnable today

CAPABILITY code exists, builds, tests pass or a document states it; no production measurement

IN DEVELOPMENT incomplete, with a named remaining gap

GATED complete, blocked on a step outside the software; the blocker class is named, the counterparty is not

TARGET forward-looking; carries a target date **ABSENT** deliberately not built or not on file; the reason is stated

EXTERNAL a third-party fact with URL, retrieval date and a verbatim quote of at most 25 words

Network: unykorn.ai · blockchainfraud.org · nil33.com · legal.unykorn.ai · our commitments