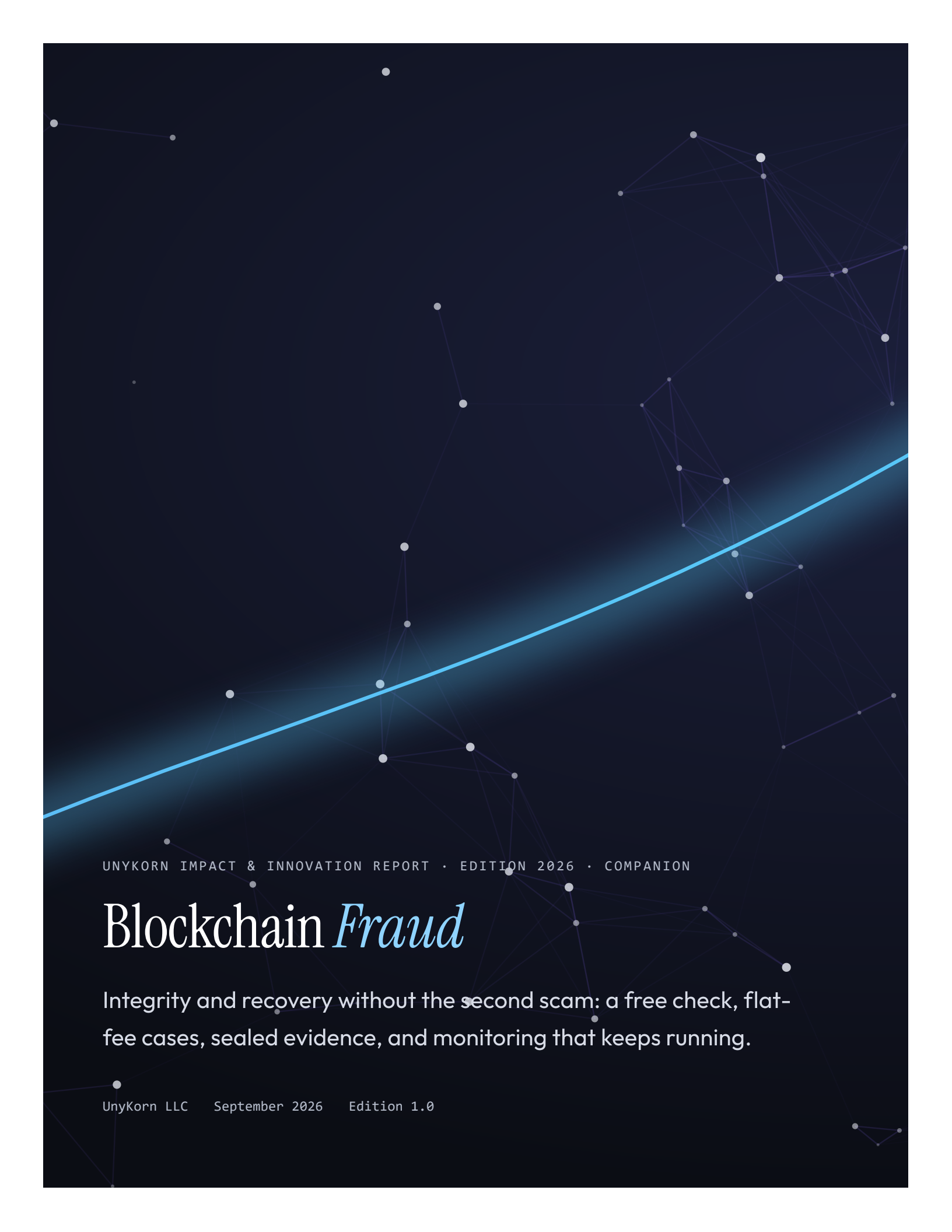




UNYKORN IMPACT & INNOVATION REPORT • EDITION 2026 • COMPANION

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 1.0

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 between September 4 and September 9, 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

"Last year saw a new record for losses reported to IC3, totaling a staggering \$16.6 billion," a 33 percent increase from 2023, from 859,532 complaints.

Cryptocurrency fraud: 149,686 complaints and \$9.3 billion in losses, a 66 percent increase, with the 60-and-over age group the largest reporting group (\$4.8 billion in losses across all crime types).

https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

EXTERNAL

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

"Misinformation and disinformation remain top short-term risks for the second consecutive year, underlining their persistent threat to societal cohesion and governance by eroding trust." Other leading short-term risks include cyber-espionage and warfare. Drawn from "over 900 global risks experts, policy-makers and industry leaders surveyed in September and October 2024"; 64% of experts anticipate a fragmented global order.

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

Sources. External sources retrieved 2026-09-09 from the URLs shown; quotations verbatim, the IMF paper paraphrased

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

43 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; the founder gets the full detail.

EVIDENCE

Vault

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

MONITORING

Watchtower API

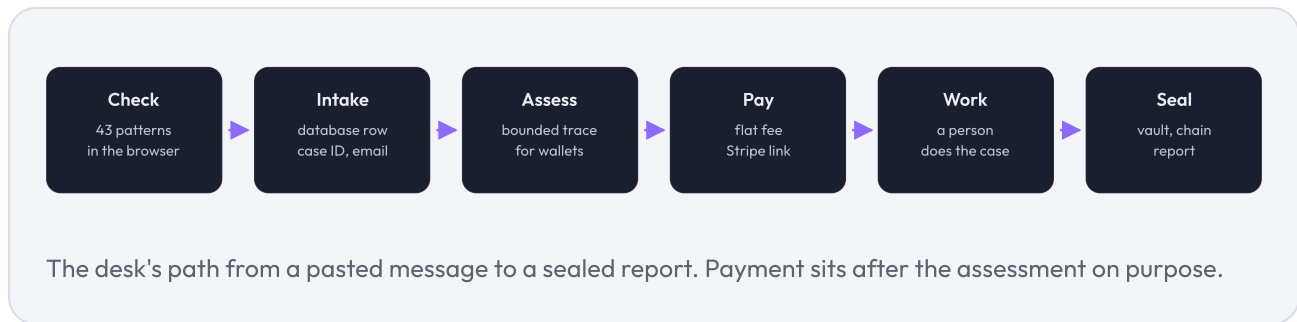
Cases, alerts, evidence-chain verification, a sweep, reports, a registry and the sanctions list on /v1/*.

REACH

Telegram bot and narrators

@blockchainfraud_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. Monitoring watches cases after they close and alerts by Telegram.

What is real today

Every row was checked against a served response or a test run on the date in the source line, not read from code.

CAPABILITY	EVIDENCE	STATE
Free scam check	Pig-butcher sample scored HIGH RISK with ranked signals; plain invoice scored INSUFFICIENT EVIDENCE; PDF library hash matches its CDN file (2026-09-09)	MEASURED
Intake and assessment	Form to database to case ID verified; assessment rendered for TRON and Ethereum-family wallets (2026-09-09)	MEASURED
Payments	Six Stripe links resolve at tier prices; /paid confirmation; REFERRED code applies the 10% customer discount (2026-09-09)	MEASURED
Evidence vault	WebCrypto-only vault script served; handler public key only; live upload verified (2026-09-09)	MEASURED
Watchtower and bot	Health, registry, sanctions (478 addresses), evidence-chain verify, a real TRON case end to end; wrong bot secret rejected (2026-09-09)	MEASURED
Full investigation automation	Runs, but the free CPU ceiling causes intermittent errors on the heaviest traces	GATED
Sealed evidence in object storage	Waits on R2 enablement; evidence sits in the database meanwhile	GATED
Named investigator byline	Not published until a real name, credential and consent exist	ABSENT
Zero-knowledge, anchoring contract, in-tab IPFS	Removed after an audit showed each proved or stored nothing	ABSENT

Trust and safeguards

The copy is scanned for the phrases we refuse to use: guaranteed, insured, licensed, immutable, tamper-proof, on-chain anchored. The site says in plain words that no recovery is promised and that a case may end with "insufficient evidence".

Credentials for the bot, Stripe and email are worker secrets. A launch-status file lists what still needs the founder's hand, including rotating bot tokens that were pasted into a chat transcript, which is exactly the kind of thing this report is for.

Economics

Flat fees, published, chosen so that a person with a \$10,000 loss and a company with a \$10 million exposure both know the price before they start.

PRODUCT	PRICE	STATE
Trace	\$750	MEASURED
Full investigation	\$1,750 retainer + \$1,750 balance	MEASURED
Security retainer	\$2,500 / month	MEASURED
Case Watch	\$249 / month	MEASURED
Cluster Watch	\$1,250 / month	MEASURED
Address screen for agents (x402)	\$0.25 per call in USDC	GATED

Next phase

Workers Paid to remove the CPU ceiling; R2 for sealed evidence; a paid block-explorer plan to add BSC, Base and Optimism to automated tracing; Gmail send-as for the case addresses; then the first quarter of published case counts in Edition 2027.

Sources. docs/LAUNCH-STATUS-2026-09-09.md (209 checks, 209 pass) · docs/REVENUE-MAP.md 2026-09-10 · docs/test-report-2026-09-08.md addenda · memory: blockchainfraud rebuild 2026-09-04 to 09-08

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 1.0, September 2026. Every figure in this report carries one of the labels below and a source line at the end of its chapter; anything without a source is marked as such. Corrections: hello@blockchainfraud.org.

MEASURED a figure taken from a served response, a test run, a filing, or a repository at a stated date

CAPABILITY something the software does today; not a count of use

IN DEVELOPMENT built, exercised, not yet on a customer surface

GATED built and waiting on an external step (a plan, a key, a verification click, counsel)

TARGET a roadmap intention, not a result **ABSENT** deliberately not built, and said so

EXTERNAL a finding quoted from a named institution, with its URL and the date we retrieved it

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