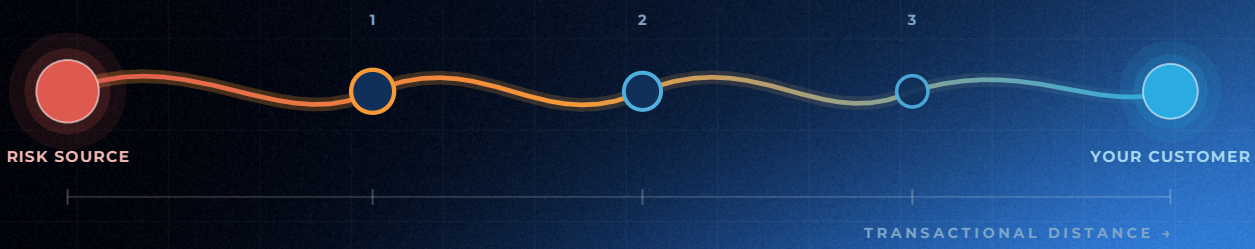
Lukka

DIGITAL ASSET COMPLIANCE

The Distance Problem.

Measuring indirect exposure in digital asset compliance — a framework for defensible risk decisions.

HOW FAR DOES RISK TRAVEL?



Published by Lukka · 2026

lukka.tech

Contents

Six Hops From a Problem 03

Risk That Moves 04

Risk Doesn’t Stop at the Address 05

Distance Is the Hard Part 06

What Goes Wrong Without a Framework 07

Two Sides of One Dial 08

A Framework for Defensible Exposure 09

How Lukka Operationalizes It 10

Distance, Made Visible 11

Direction and Distance, Quantified 12

A Foundation Built to Be Defended 13

Questions Every Institution Should Ask 14

FOREWORD

Six Hops From a Problem

Why indirect exposure sits at the center of nearly every crypto AML decision.

A compliance analyst at a regulated institution opens the morning alert queue. A customer's wallet has been flagged: it received funds that, several transactions earlier, passed through a sanctioned mixer. The address itself is not sanctioned. The customer is not a criminal. But somewhere upstream, the money touched something toxic.

Now the analyst has to make a decision that an auditor, and possibly a regulator, will later review. Is this exposure material? Should the account be frozen? Is a suspicious activity report warranted? Or is this one of the hundreds of low-relevance alerts that will consume the team's week and, in the end, mean nothing?

The honest answer is that it depends almost entirely on methodology the analyst usually cannot see. How was “exposure” measured? How far does risk travel before it stops mattering? Was the flag driven by a direct, verifiable link, or by a probabilistic guess propagated across an unverified cluster of addresses? Two analytics tools can examine the same wallet and return very different verdicts, and the difference is rarely visible in the score itself.

This is the **distance problem**. It is the single most common source of both wasted effort and missed risk in digital asset compliance — the reason good teams drown in false positives and, at the same time, miss the exposure that actually mattered. It is also entirely solvable, but only with a methodology that is decomposable, traceable, and built to be questioned.

This paper defines the problem, explains why it is genuinely hard, sets out what a defensible approach requires, and ends with the questions every institution should be able to ask of its own analytics, and get a straight answer.

> **THE CORE QUESTION**
>
> In digital assets, the compliance question is no longer simply “is this address risky?” It is **“how much risk reaches this address, from how far away, and how confident are we in the link?”**

EXECUTIVE SUMMARY

Risk That Moves

Blockchain's transparency is what makes compliance possible — and deceptively hard.

Every transaction on a public ledger is visible and permanent. That transparency is the foundation of digital asset compliance, and the reason it does not behave like traditional financial crime control. Because funds move freely, publicly, and continuously, **risk does not stay put**. A wallet that is clean today can be one transaction away from a sanctioned counterparty tomorrow. Risk in crypto is relational, not merely local.

WHAT THIS PAPER ARGUES

1. **Screening an address in isolation misses the point.** Most consequential AML questions concern exposure that arrives through an address's transaction history, not the address itself.
2. **"Exposure" conflates several distinct claims.** Direct involvement, owner risk, and inherited (indirect) risk carry different evidence and different consequences. Collapsing them into one number is how good teams make indefensible decisions.
3. **Distance is the hard variable.** Risk decays with transactional distance — but not uniformly — and mixers, bridges, and peel chains are engineered specifically to break the trail.
4. **Without a framework, institutions fail in one of two directions:** alert fatigue (flag everything, defend nothing) or blind spots (miss the exposure that mattered).
5. **A defensible approach is decomposable, directional, distance-aware, traceable, and continuous** — and it must survive an auditor's simplest question: "why did you conclude that?"

WHY THIS MATTERS NOW · 2026

The bar for demonstrable controls has risen sharply. In the EU, **MiCA** is now fully applicable and the **Transfer of Funds ("Travel Rule")** regulation has been enforceable since December 2024; the EU's Anti-Money Laundering Authority (**AMLA**), operational since mid-2025, has been explicit that it expects **evidence in a system, not assurances in a policy**. In the U.S., the **GENIUS Act** (2025) brought payment stablecoins under the Bank Secrecy Act. Globally, **FATF** continues to press Travel Rule adoption, with a majority of surveyed jurisdictions now having enacted implementing legislation. Across every regime, supervisors are converging on the same expectation: risk decisions must be **current, traceable, and defensible**.

Risk Doesn't Stop at the Address

Direct exposure is a lookup. Indirect exposure is where the real difficulty — and the real value — lives.

Traditional financial-crime controls were built around identifiable parties: a named sender, a named beneficiary, a bank in between. Digital assets break that model. On a public ledger, a counterparty is an **address** — a string of characters with no inherent identity — and value flows between addresses continuously, permissionlessly, and at global scale.

This produces two distinct kinds of risk that institutions must assess, and that are dangerously easy to conflate:

Direct exposure

The address, or its owner, is **itself** the source of concern: it appears on a sanctions list, belongs to a known illicit service, or is directly involved in a hack, ransomware campaign, or fraud scheme.

Indirect exposure

The address is clean on its own, but its funds **originated from, or flowed toward**, a risky counterparty, one or more transactions away. The risk is inherited through the transaction graph.

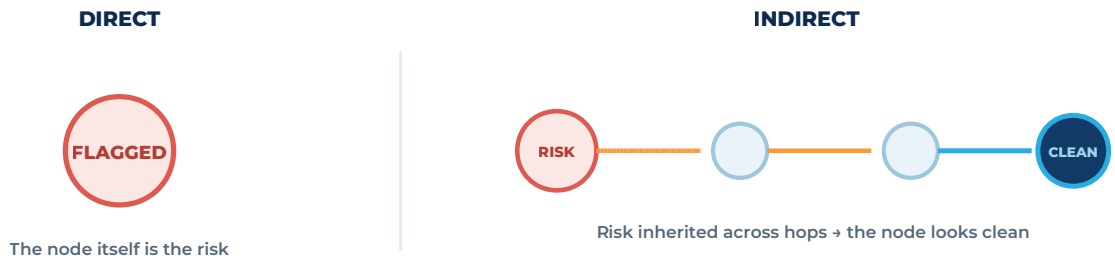


Fig. 1 — The same “clean” wallet can carry material inherited risk that address-level screening never sees.

Direct exposure is comparatively tractable: it is a lookup against attributed, verified data. **Indirect exposure is where the difficulty lies**, and where nearly every consequential question actually sits. Did this deposit ultimately originate from a sanctioned entity? Is a customer unknowingly receiving the proceeds of a hack? Is our exchange being used as an off-ramp for funds laundered three hops upstream?

Answering these requires tracing value across the ledger and quantifying how much risk propagates along the way. That process — **risk propagation** — is the engine of crypto AML. It is also where methodology quietly determines the outcome.

Distance Is the Hard Part

Risk propagation, attenuation, and deliberately adversarial obfuscation.

If every risky dollar contaminated everything it ever touched — equally, and forever — compliance would be simple, and useless. Every wallet on a public chain is, at some remove, connected to something bad. A method that treats all exposure as equal flags the entire ecosystem and tells you nothing.

The reality is that **risk attenuates with distance**. Funds one hop removed from a sanctioned address carry very different weight than funds that passed through fifty intermediaries, over months, mixed with legitimate flows the entire way. The central methodological task is to measure that attenuation — to answer, defensibly: how far does risk travel before it stops being material to this decision?

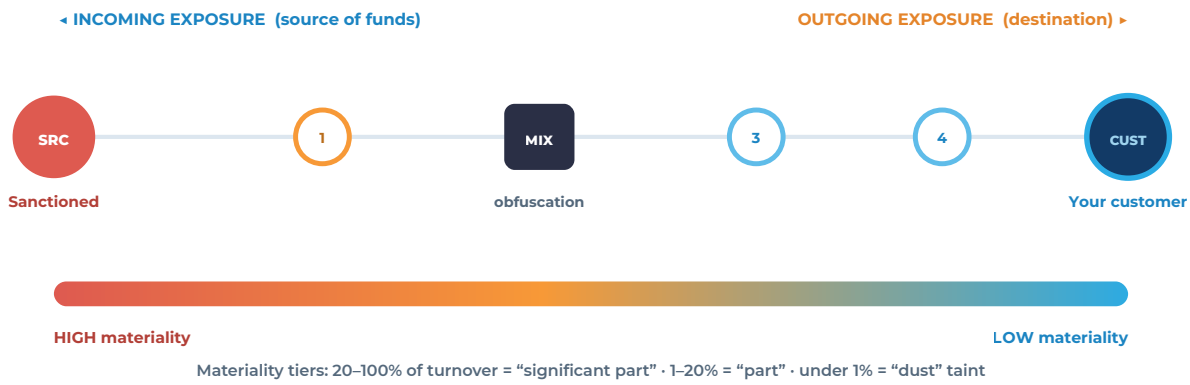


Fig. 2 — Measuring inherited risk means accounting for direction, distance, and deliberate concealment at once.

Three properties make this genuinely difficult:

Direction matters

Incoming exposure (source of funds) and **outgoing** exposure (destination) are different questions with different regulatory weight, and a serious framework measures them separately.

Proximity is policy

How many hops are "too many" depends on jurisdiction, asset, and risk appetite. A threshold that is **hard-coded or hidden** cannot be tuned, defended, or reproduced.

Obfuscation is adversarial

Mixers, bridges, and peel chains exist to sever the source-to-destination link. A naive tracer loses the trail, and reports **"no exposure"** exactly where it is most likely.

The distance problem, then, is not a single calculation but a discipline: measuring inherited risk across a transaction graph — with direction, tunable proximity, and resilience to concealment — in a way a third party can inspect and trust, and that stays current as the rules themselves shift, as the 2025 delisting of a prominent mixer showed.

What Goes Wrong Without a Framework

Five failure modes of undisciplined exposure measurement. Most institutions experience several at once.

1 **Alert fatigue — the false-positive flood** OVER-FLAGGING

Set exposure thresholds too broadly, or ignore distance entirely, and nearly everything lights up. Analysts drown in low-relevance alerts, the genuinely urgent ones are buried, and the program's credibility erodes. Over-flagging is not caution — it is a different way of failing.

2 **Blind spots — the false-negative gap** UNDER-FLAGGING

Set thresholds too narrowly, or use a tracer that cannot see through mixers and bridges, and real exposure passes unnoticed. The most dangerous alert is the one that never fires — the sanctioned-origin deposit that was three hops too far, or one bridge crossing away, to be caught.

3 **The black-box score** NOT DEFENSIBLE

A single risk number with no visible basis cannot be defended. When an auditor asks “why is this a 99?”, “unexplained model output” is not an answer. If the path from evidence to conclusion is not inspectable, the decision is not defensible, regardless of whether it happened to be correct.

4 **Static-screening blindness** POINT-IN-TIME

A wallet screened once, at onboarding, and never again reflects the risk of a single moment. But exposure is dynamic: the customer who was clean at onboarding may receive tainted funds next week. Point-in-time screening in a continuously moving system is a structural blind spot.

5 **Guesswork dressed as fact** UNEXAMINED INFERENCE

When probabilistic outputs — statistical inference, machine-learning predictions — are merged into the same score as deterministic, verifiable links, with no way to tell which is which, a plausible guess and a proven fact become indistinguishable. That is precisely the ambiguity that collapses under cross-examination.

SECTION 3 · THE TRADE-OFF

Two Sides of One Dial

Turn sensitivity up and you get alert fatigue; turn it down and you get blind spots.

The first two failure modes are not opposites to be chosen between. They are two readings on the same dial. Every institution sets its exposure sensitivity somewhere, whether deliberately or by default. Set it loose and false positives flood the queue; set it strict and real risk slips through. The goal is not a magic setting. It is a framework that makes the trade-off **explicit, tunable, and explainable**, so the chosen point can be justified to a regulator rather than merely inherited from a vendor's defaults.

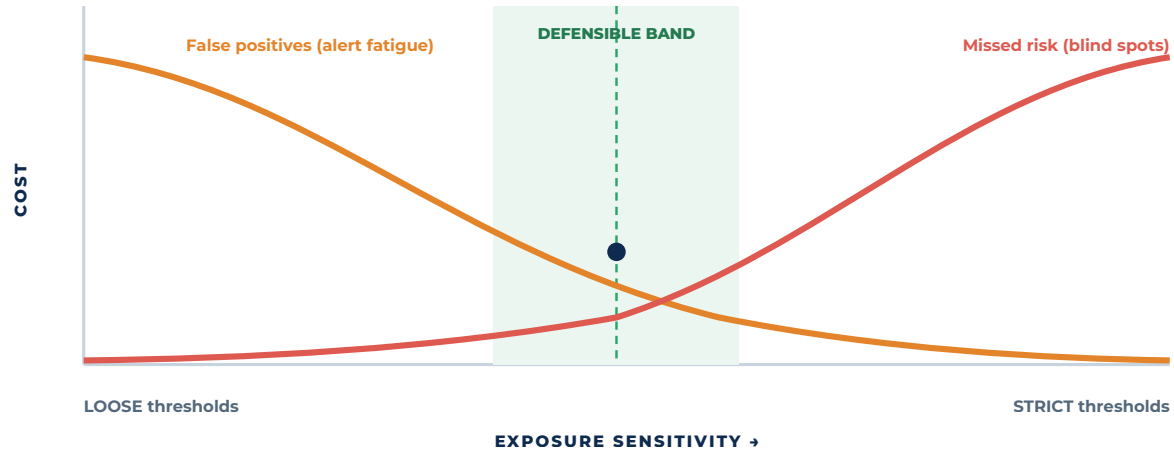


Fig. 3 — A rigorous methodology does not hide the trade-off; it exposes the dial and lets policy set the point.

Turn it too loose

Thresholds flag nearly everything. Analysts drown in low-relevance alerts, the genuinely urgent cases are buried, and the program's credibility erodes with every false alarm.

Turn it too strict

Real exposure slips through. A sanctioned-origin deposit a few hops away never trips an alert, and the miss surfaces only later, in an audit or an enforcement action.

Reaching that defensible band is not a matter of a single clever algorithm. It requires a set of commitments, the framework that follows.

A Framework for Defensible Exposure

Five principles that make an indirect-exposure decision defensible — to an auditor, a regulator, or a court.

Measuring indirect exposure well is a discipline, not a feature. Lukka builds to the following five principles — a baseline any institution can hold its analytics to, its vendors' and its own.

1

Decompose the risk

Separate **direct involvement**, **owner / entity risk**, and **inherited (indirect) risk**, and report each on its own terms. A score that cannot be broken back down into its components cannot be examined, or trusted.

2

Anchor on deterministic, attributed data

The foundation must be verifiable: attributions built on evidence, not inference, so a link between an address and an entity can be reproduced and stood behind. Probabilistic methods have a role — surfacing leads, spotting patterns — but they belong on top of a deterministic foundation, clearly labeled, never silently fused into it.

3

Make distance and direction explicit

Measure **incoming** and **outgoing** exposure separately, quantify exposure by proximity (hops), and expose those parameters so they can be tuned to jurisdiction, asset, and risk appetite — and justified afterward.

4

Trace to the source — and show the path

Every material exposure should resolve to a specific origin, with the route from counterparty to risk source visible and inspectable. “There is exposure” is a claim; **“here is the path to it” is evidence.**

5

Screen continuously, not once

Risk is a moving target; controls must move with it. Onboarding screening sets a baseline; ongoing monitoring and re-scoring keep it current as new transactions occur, with alerts when a wallet's risk profile changes.

Beneath all five: explainability. If a compliance officer cannot answer “why did the system conclude this?” in language an auditor accepts, the tool has not done its job, however sophisticated its internals.

SECTION 5 · FROM FRAMEWORK TO WORKFLOW

How Lukka Operationalizes It

Principles matter only if they run in production, across the full compliance lifecycle.

Lukka Blockchain Analytics implements this framework end to end — onboarding, monitoring, investigation, and reporting — on a foundation of deterministic, institutional-grade data spanning blockchains that represent **99%+ of crypto market capitalization**, with **1.2B+ deterministically attributed addresses** and **380+ risk indicators** across sanctions, terrorism financing, hacks, ransomware, and on-chain behavior.



ONBOARD · AML RISK REPORTS

A defensible client risk profile at KYC

Establish who a counterparty is, what they do, who controls them, and the source of their funds, with direct, owner-level, and inherited risk scored **separately**, then merged into one explainable **C-Score** (0–99). Delivered via Web UI, PDF, and API.

MONITOR · MONITORING PANEL + API

Continuous, automated screening

Ongoing screening of deposits, withdrawals, and activity across **109+ blockchains** and **50M+ transactions daily**, with real-time alerts when a wallet's exposure or rating changes, plus withdrawal pre-screening that can block a transfer to a suspicious address before it settles.

INVESTIGATE · OMNI + INVESTIGATOR

Trace source and destination of funds

Follow funds across chains and hundreds of consecutive transactions, with visibility into **50,000+ entities**, de-mixing and bridge-decoding to see through obfuscation, and configurable tracing methods — **FIFO, LIFO, PRO RATA, TAINT LAST** — for defensible attribution.

REPORT · CASE MANAGEMENT

Audit-ready documentation

Document the investigation, attach evidence, apply four-eyes supervisory review, and export audit-ready reports for internal governance, regulators, or SAR filing.

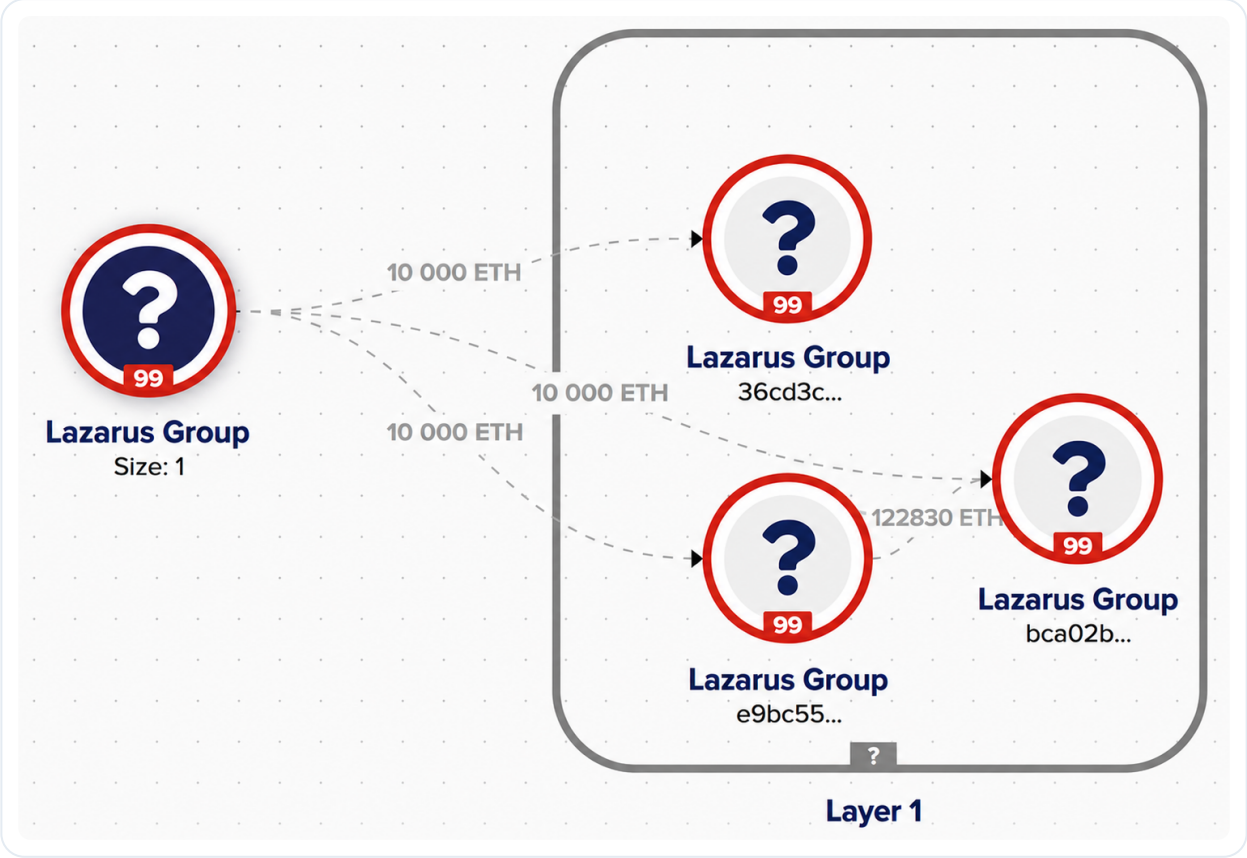
THE PAYOFF

Because the foundation is **deterministic** and every exposure resolves to a **traceable source**, the output is not just a score: it is a defensible, reproducible answer to the auditor's question. Automated tracing has been shown to make investigations **up to 60% more efficient**, freeing analysts to focus on judgment rather than manual graph-walking.

Distance, Made Visible

The framework in this paper is not theoretical: it is how Lukka Blockchain Analytics works.

Indirect exposure is not an abstraction. In the platform it is a graph, with value moving from a flagged source outward, hop by hop. Every address is independently scored and every transfer preserved, so an analyst can see not just that exposure exists, but exactly how it arrived.



Risk propagates across hops. Funds move from a flagged source through intermediary addresses, each node independently scored and each transfer preserved. Exposure is not a property of a single address; it travels along the path, and the path stays inspectable.

Direction and Distance, Quantified

The same discipline governs how exposure is measured, not just how it is traced.

Direct involvement is separated from indirect, incoming exposure from outgoing, and the distance the analysis reaches is a control the institution sets, not a black-box default. The result is an exposure profile that maps directly to the principles in this paper.



Direction and distance are measured, not assumed. Indirect exposure is quantified by counterparty type, with incoming and outgoing exposure reported separately and a tunable distance (hops) control, the paper's principles made operational and configurable.

LUKKA BLOCKCHAIN ANALYTICS · BY THE NUMBERS

A Foundation Built to Be Defended

Deterministic, institutional-grade coverage, the substrate every exposure calculation rests on.

99%+

of crypto market capitalization covered, by blockchain

1.2B+

deterministically attributed addresses

380+

risk indicators: sanctions, terrorism financing, hacks, ransomware & more

50M+

transactions screened daily across 109+ blockchains

50K+

real-world entities identified for counterparty analysis

4

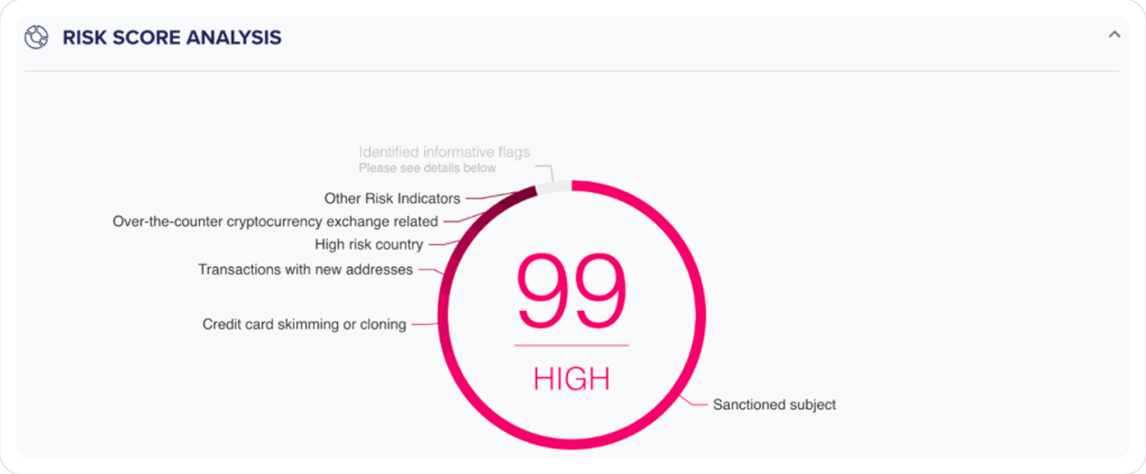
configurable tracing methods: FIFO · LIFO · PRO RATA · TAINT LAST

Knowledge-based, deterministic layer

Ownership & clustering, risk propagation, and transactional / behavioral analysis, auditable analyses that form the **structural foundation** of every score.

Risk-based layer, clearly bounded

Statistical and machine-learning signals extend reach and surface leads, layered **on top of** the deterministic foundation, never silently fused into it.



The score is explainable by design: a 99 (HIGH) resolves to the specific indicators behind it, so an analyst or auditor can see exactly why.

Questions Every Institution Should Ask

A due-diligence checklist for indirect-exposure methodology, no proprietary disclosure required.

The fastest way to assess any blockchain analytics capability, a vendor's or your own, is to ask how it handles indirect exposure. These questions simply ask a provider to describe the nature of its claims. A rigorous approach welcomes them.

FOUNDATION

- ☑ Is your attribution **deterministic and reproducible**, or inferred? Can a link between an address and an entity be independently reconstructed?
- ☑ Can you separate **direct, owner, and inherited risk**, or is exposure a single fused number?

DISTANCE & DIRECTION

- ☑ Do you measure **incoming and outgoing** exposure separately?
- ☑ Is **proximity (hops)** configurable to our jurisdiction, assets, and risk appetite, and is the setting visible?

OBFUSCATION & COVERAGE

- ☑ Can your tracing **see through mixers, bridges, and peel chains**, or does the trail end there?
- ☑ Do you cover the **chains and assets** our customers actually use?

EXPLAINABILITY & CURRENCY

- ☑ For any exposure, can you show the **path to the risk source**?
- ☑ Do you **re-screen continuously** and alert when a wallet's risk changes after onboarding?
- ☑ Could this decision withstand a regulator's or auditor's simple **“why?”**

> **If a provider cannot answer these plainly, the gap is not academic. It is the gap between a decision you can defend, and one you cannot.**

Lukka

Trust. Truth. Transparency.

Digital assets are becoming financial infrastructure, and the institutions adopting them are held to institutional standards. Meeting those standards takes more than a risk score. It takes data you can **verify**, methodology you can **explain**, and controls that keep pace with a market that never stops moving.

That is the standard Lukka is built to — a leading provider of institutional-grade data, software, and analytics for the digital asset industry, helping financial institutions, exchanges, regulators, auditors, and compliance teams navigate digital assets with trusted data, audit-ready infrastructure, and defensible reporting.

Trust

Enterprise-grade systems, controls, and audit readiness.

Truth

Accurate, normalized, verified digital asset data.

Transparency

Clear lineage and visibility across on-chain and off-chain activity.

lukka.tech

Building the institutional standard for digital assets

This material is for informational purposes only and does not constitute legal, tax, financial, compliance, or investment advice. Regulatory references reflect information available as of 2026 and are subject to change; institutions should verify current requirements with qualified advisors. Product capabilities, coverage figures, and statistics are described at a general level, are drawn from Lukka product materials, and may change without notice. © 2026 Lukka, Inc. All rights reserved.