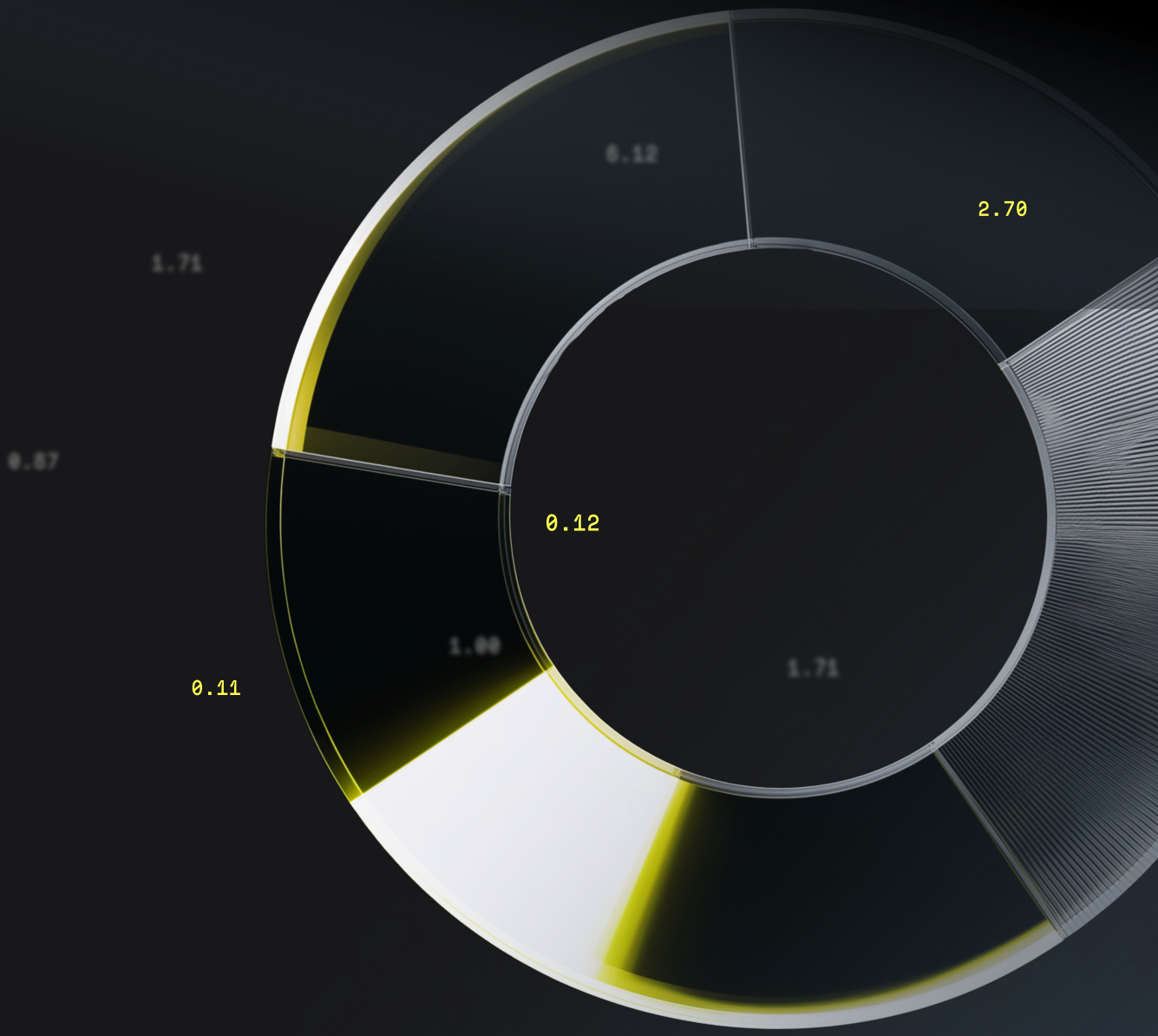
Crystal Intelligence



Nested Services

The $8 billion compliance blindspot

SERIES
Compliance Blindspots

AUDIENCE
Regulators, Compliance, Law Enforcement

PUBLISHED
August 2026

Table of Contents

At a glance 3
Executive summary 4
The compliance blind spot 5
Why this matters 8
Research methodology: summary 9
How large is the problem? 10
- Global nested service landscape 10
- Annual transaction volume and entity count (2017-2025) 11
- Token patterns and transaction count analysis 12
- Top nested entities by volume 15
- Multi-host entities 16
- Geographic concentration 16
- Iran-attributed nested services 19
- Two exchanges anchor the Iran cluster 20

What does the problem look like? 20
Detecting nested services 24
- Using AI agents to spot nested services 26
- Attribution confidence levels 27

Closing the blind spot 28
- Five primary risk areas 28
- Recommendations by audience 29
- About Crystal Intelligence 29

Appendix 30

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

At a glance

This report in brief, for readers who need the headline numbers before the full analysis:

01	$8B traced in nested-service volume across 39 host exchanges, 2017-2025 (2,275,270 transactions).
02	87% of that volume concentrates in a single host exchange.
03	17 entities in the Iran sanctions cluster, $239M total, subject to OFAC sanctions.
04	Entities are labeled NS-01 through NS-34 in this version — codes are unique across the whole report and are never reused, so a code always means the same entity (see “How entities are labeled” in Section 3).
05	Exchange-level monitoring cannot see these operators; entity-level attribution can (Section 6).

HOW TO USE THIS REPORT

Host exchange compliance teams should start with Section 6 (Detecting Nested Services) and the host-exchange recommendations in Section 7. Regulators and FIUs will find Section 2 (Why This Matters) and the regulator recommendations in Section 7 most directly relevant. Correspondent banks and payment processors should read Section 2 alongside the correspondent-banking recommendations in Section 7. Short on time: read the Executive Summary, then go straight to Section 7.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Executive summary

Nested services are third-party platforms that conduct business through accounts held at other exchanges, effectively inheriting their compliance infrastructure while operating with far less oversight. The result is a structural compliance blind spot that presents material risks to regulated financial institutions, correspondent banks, and jurisdictions reliant on those exchanges for transaction monitoring.

The Financial Action Task Force (FATF) echoed this in its seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs (July 16, 2026): offshore VASPs opening accounts on licensed platforms, misrepresenting themselves as retail users, then processing illicit transactions that significantly exceed typical retail volumes while accounting for only a marginal share of the host platform's total activity. FATF calls this a nested and intermediated arrangement, and recommends enhanced due diligence on offshore VASPs, detection of accounts that misrepresent themselves as retail, restricting or exiting higher-risk relationships, and monitoring fiat on- and off-ramp activity tied to unlicensed or weakly supervised platforms. That recommendation assumes compliance teams can see the thing being described. Most can't. That’s the gap this report closes.

Nicholas Smart

Chief Intelligence Officer, Crystal

"The continued growth of digital asset adoption - particularly among financial institutions and regulated businesses - makes it increasingly important to identify and address compliance blind spots. As the ecosystem matures, market participants need a legal and trusted environment in which to operate, supported by robust risk management, transparency, and effective compliance practices.

Research that sheds light on emerging challenges, such as nested services, contributes to a better understanding of the risks and encourages informed discussions across the industry. Combined with advances in blockchain analytics and greater regulatory clarity, this helps strengthen trust in the digital asset ecosystem and supports its sustainable growth

Mirela Ciobanu

Lead Editor, Banking & Fintech.
The Paypers

the paypers

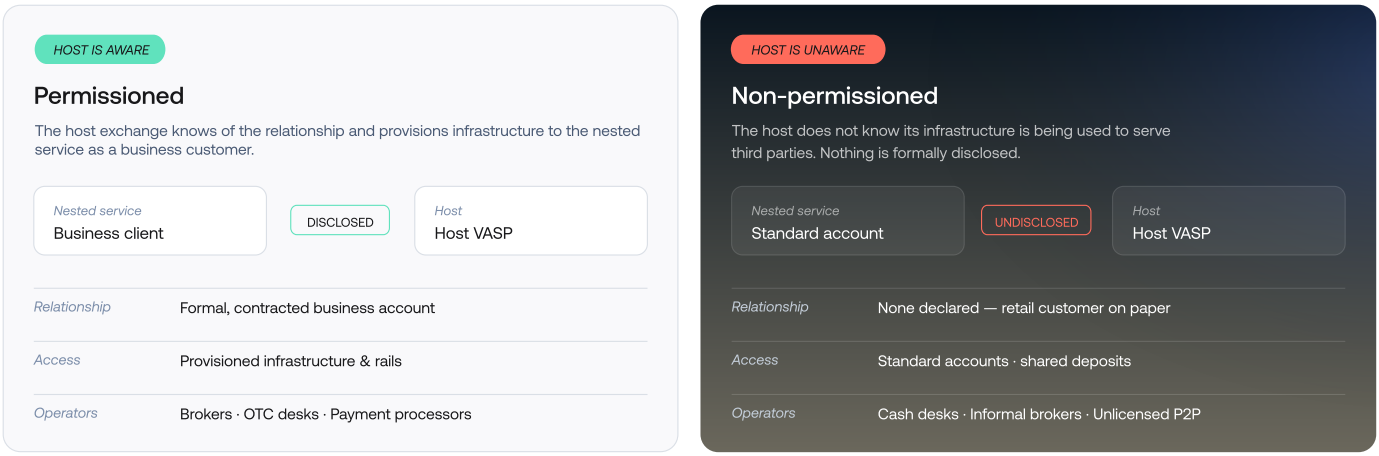
Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

THE PROBLEM

The compliance blind spot

A nested service is a crypto exchange, broker, OTC desk, payment processor, or other virtual asset service provider (VASP) that operates through accounts or wallet infrastructure provided by a larger exchange, custodian, or payment processor rather than maintaining its own independent blockchain infrastructure.

Two models — and only one where the host knows



Above: In both models the host's KYC stops at the account holder — but only in permissioned arrangements does the host know a third-party client base exists behind it. Source · Crystal Intelligence

Nested arrangements are either permissioned, where the host knows of the relationship and provisions infrastructure to the nested service as a business customer, or non-permissioned, where the host is unaware its infrastructure is being used to serve third parties and nothing is formally disclosed.

Nested structures are not inherently illicit — many legitimate businesses rely on host infrastructure to access liquidity, custody, payment rails, or local markets without building their own — but the same model can be exploited by sanctioned entities, darknet marketplaces, and other illicit actors seeking to use the host's infrastructure while obscuring their own identity.

The compliance gap is equally important: host exchanges typically have limited or no visibility into a nested service's own end customers, products, or services, even where their own KYC/KYB and monitoring controls are highly robust.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Service categories

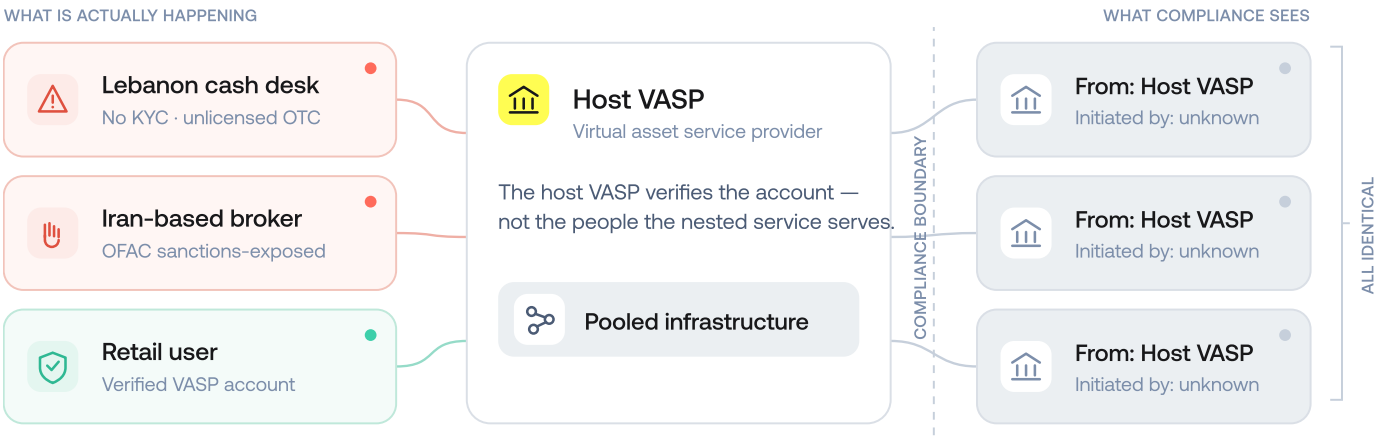
Nested arrangements fall into three operating models.

- A host controls the wallets, private keys, and on-chain execution, and may perform KYB on the nested service, but has no visibility over its end users.
- The nested service is the customer-facing layer: it manages branding and onboarding but doesn't control custody, and is rarely licensed.
- A hybrid model partially controls its own infrastructure while routing specific flows through a host, creating the highest attribution complexity of the three.

CATEGORY	ROLE	COMPLIANCE IMPLICATION
Host Infrastructure provider	Controls wallets, private keys, custody and on-chain execution. May perform KYB on the nested service but has no visibility over end users.	Inherits indirect exposure to all downstream nested-service clients and their user bases.
Nested service Front-end	Customer-facing layer. Manages the user relationship, branding and onboarding. Does not control private keys or custody.	Rarely licensed. May impose no KYC — operating inside the host's compliance perimeter without matching its standards.
Hybrid model Nested & host	Partially controls own infrastructure while routing specific flows through a host. Includes multi-tier nesting — simultaneously nested and a host to downstream services.	Maximum attribution complexity. Layered accountability gaps across multiple tiers.

Above: The three operating models and what each one hides from the host. Source: Crystal Intelligence

The compliance blind spot created by nested services



A withdrawal from the host VASP's infrastructure may be initiated by the Lebanon cash desk or the Iran broker — but that initiator is never visible on-chain. Every transaction shows the same counterparty: the host VASP.

Above: Three different originators, one indistinguishable transaction record. Source: Crystal Intelligence

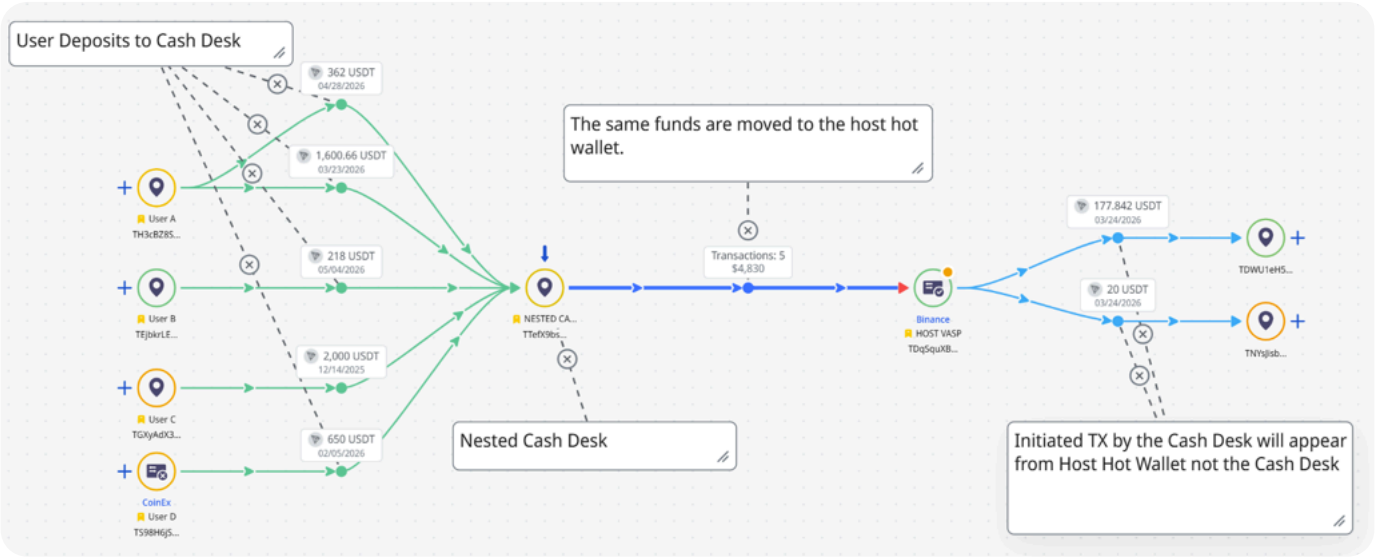
Source · Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

The core compliance problem is that transactions routed through nested services are indistinguishable from transactions executed by the host exchange itself. A host exchange may apply robust KYC, KYB, transaction monitoring, and sanctions controls to the nested service as its direct customer, while having little or no visibility into the nested service's own end users, products, or service delivery methods (which may apply much weaker controls, or none at all).

A second risk arises from the host's own regulated infrastructure: it can be used to process activity from customers who would not have met the exchange's onboarding or monitoring standards if they had interacted with the exchange directly.

For example, a transaction appearing to originate from the host exchange may have been initiated by a nested cash desk in Lebanon operating without KYC, or by a broker in Iran routing customer funds through the exchange's deposit infrastructure — and to analytics providers, financial institutions, and counterparties, it appears to originate from the regulated host, obscuring the true source of the activity.



Above: An example transaction appearing to originate from the host exchange may have been initiated by a nested cash desk in Lebanon operating without KYC. Source Crystal Expert

Regulatory requirements such as the EU's Markets in Crypto-Assets Regulation (MiCA) raise the stakes: a compliance team that treats a transaction from a known, licensed exchange as inherently low-risk has no mechanism to identify a nested operator in a high-risk jurisdiction behind it.

Entity-level attribution is the mechanism that makes this distinction visible, particularly since Travel Rule data may show only a natural person as originator, with no indication a service provider sits behind the account.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 2

Why this matters

Nested-service risk does not land the same way for everyone:

AUDIENCE	WHY THIS MATTERS
Host exchanges	Nested accounts hide their own end customers from you. The KYC/KYB and sanctions screening you would apply to a direct customer never reaches the people actually transacting through a nested account.
Regulators	Beneficial-originator visibility drops sharply once activity routes through a nested layer — even at exchanges with strong direct-customer controls — making licensing and enforcement assessments harder to get right.
Banks & payment processors	A correspondent relationship with a crypto exchange client carries counterparty risk the exchange's own compliance program does not cover — because that program was never built to see inside its own nested accounts.
Compliance teams	Exchange-level monitoring reads nested activity as routine. That creates false confidence that a real risk has already been checked, when in fact it was never visible in the first place.

Above: How nested-service risk reaches each audience. Source: Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 3

Research methodology: summary

All entities in this report are confirmed as active services unless otherwise noted; Crystal Intelligence does not include suspected entities without corroborating evidence.

The analysis draws on Crystal Intelligence's attribution database — Bitcoin, Ethereum, Tron, Litecoin, Stellar, and other represented chains — spanning January 2017 through December 2025, covering 2,052 wallet addresses attributed to identified nested-service entities via Crystal's dual tag/label model (tagging the nested service, labeling the controlling host).

Volumes represent gross throughput, not netted internal transfers. This report captures only nested services identified by Crystal; the true population is likely larger.

How entities are labeled

- Every nested entity in this report is assigned a unique code — NS-01 through NS-34 — the first time it appears.
- No code is ever reused, so a given code always refers to the same entity everywhere in this document, in every table, and in every section.
- Host exchanges keep their existing labels (“Tier-1 Global Exchange (Host A),” etc.), which are likewise consistent throughout: the same letter always identifies the same host. SUEX is named directly rather than coded, since it was already publicly identified by OFAC's 2021 sanctions designation (Section 5, Case study 4).

Full scope, chain coverage, and volume methodology are in the Appendix.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 4

How large is the problem?

The findings point to a broader AML challenge: host exchanges may have limited visibility into the underlying customers of nested services, creating blind spots that exchange-level monitoring alone will not catch. Closing that gap calls for enhanced nested-service detection, mandatory disclosure obligations, and targeted risk-based monitoring by host exchanges and their regulators.

$7.97B	39	87.4%	2,275,270
Total nested-service volume traced	Host exchanges routing the flows	Of all volume hosted by Host A alone	Transactions, 2017–2025

Above: The nested-service landscape at a glance. Source: Crystal Intelligence

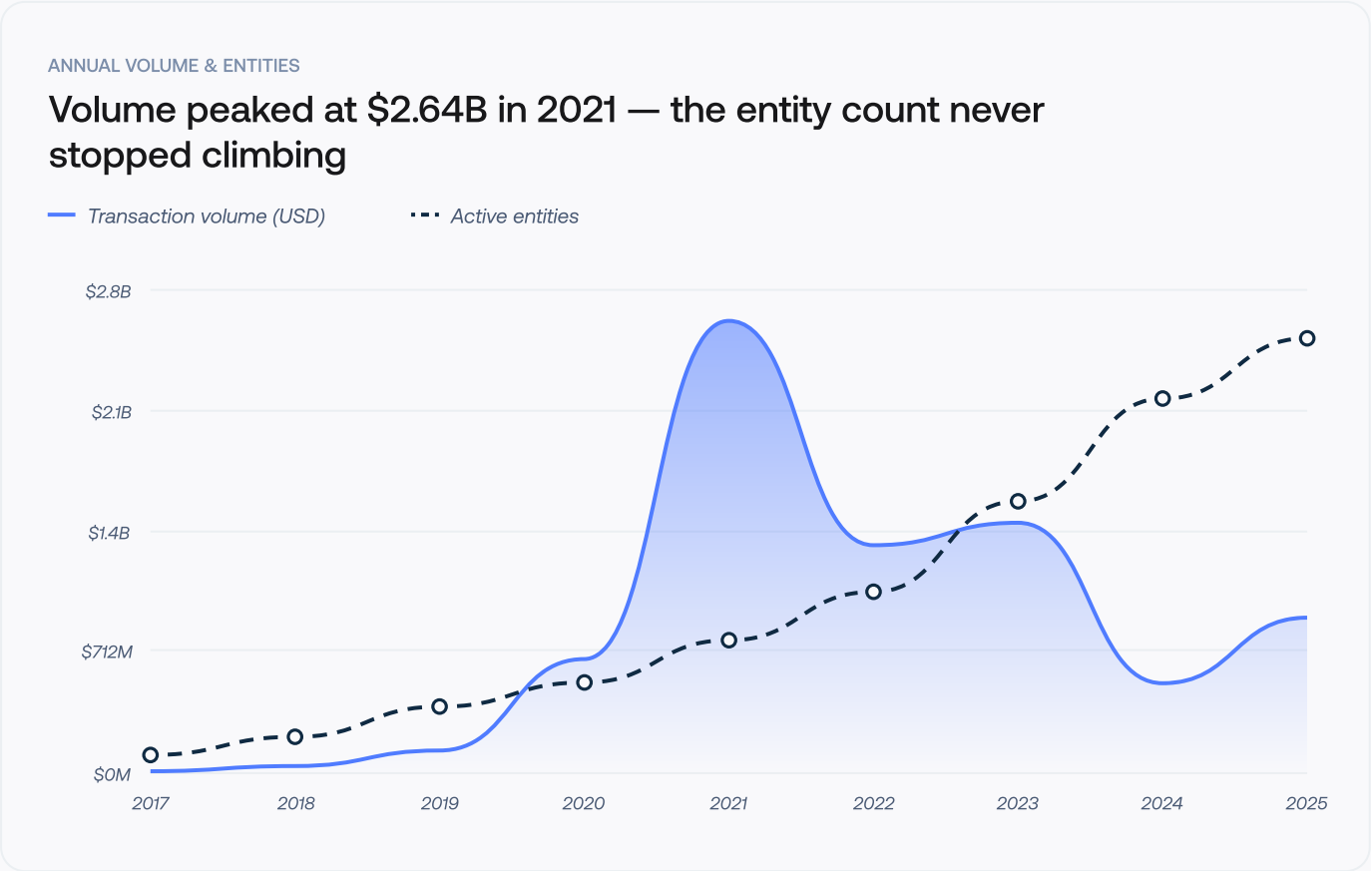
Global nested service landscape

Crystal Intelligence identified a population of distinct nested service entities operating across 39 host exchanges, with a combined on-chain transaction volume of $8B between 2017 and 2025:

ENTITY	VOLUME	HOST(S)	STATUS
NS-01	$2.84B	Host A	Licit, instant-swap
NS-02	$2.64B	Host A + Host D	Licit, instant-swap
NS-03	$371.3M	Host A	Unlicensed, high-risk (Case study 1)

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Annual transaction volume and entity count (2017-2025)



Above: Annual transaction volume and active entities, 2017–2025

Volume peaked in 2021 at $2.64B, driven by NS-01 and NS-02 during the broader crypto bull market; the 2022 decline likely reflects the wider market contraction, and the 2023–2025 recovery may partly reflect newly identified entities and increased stablecoin activity.

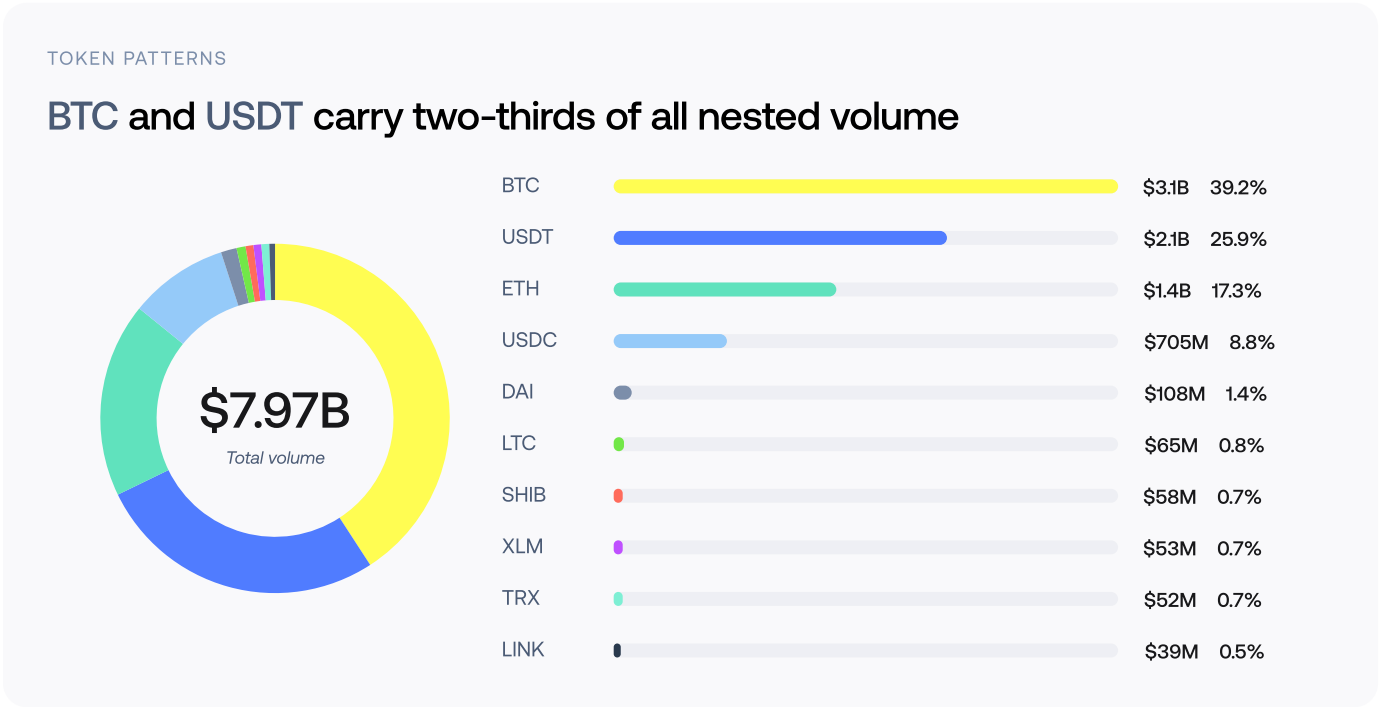
Entity count grew steadily throughout, reflecting the continued expansion of the nested-service ecosystem as nested infrastructure lowers the barriers to entry for exchanges, brokers, cash desks, and payment processors that would otherwise need to build their own.

That said, rising regulatory scrutiny, stronger host due diligence, and mandatory disclosure requirements could make hosted arrangements less attractive going forward, even as some operators migrate toward self-custodial infrastructure.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Token patterns and transaction count analysis

BTC accounts for 39.2% of total volume ($3.13B); stablecoins (USDT, USDC, DAI) collectively add another ~36.1%, reflecting their role in cross-border payments and routine settlement. The two patterns coexist: high-value, low-frequency settlement alongside high-frequency payment flows.



Above: Token patterns: BTC and USDT dominate

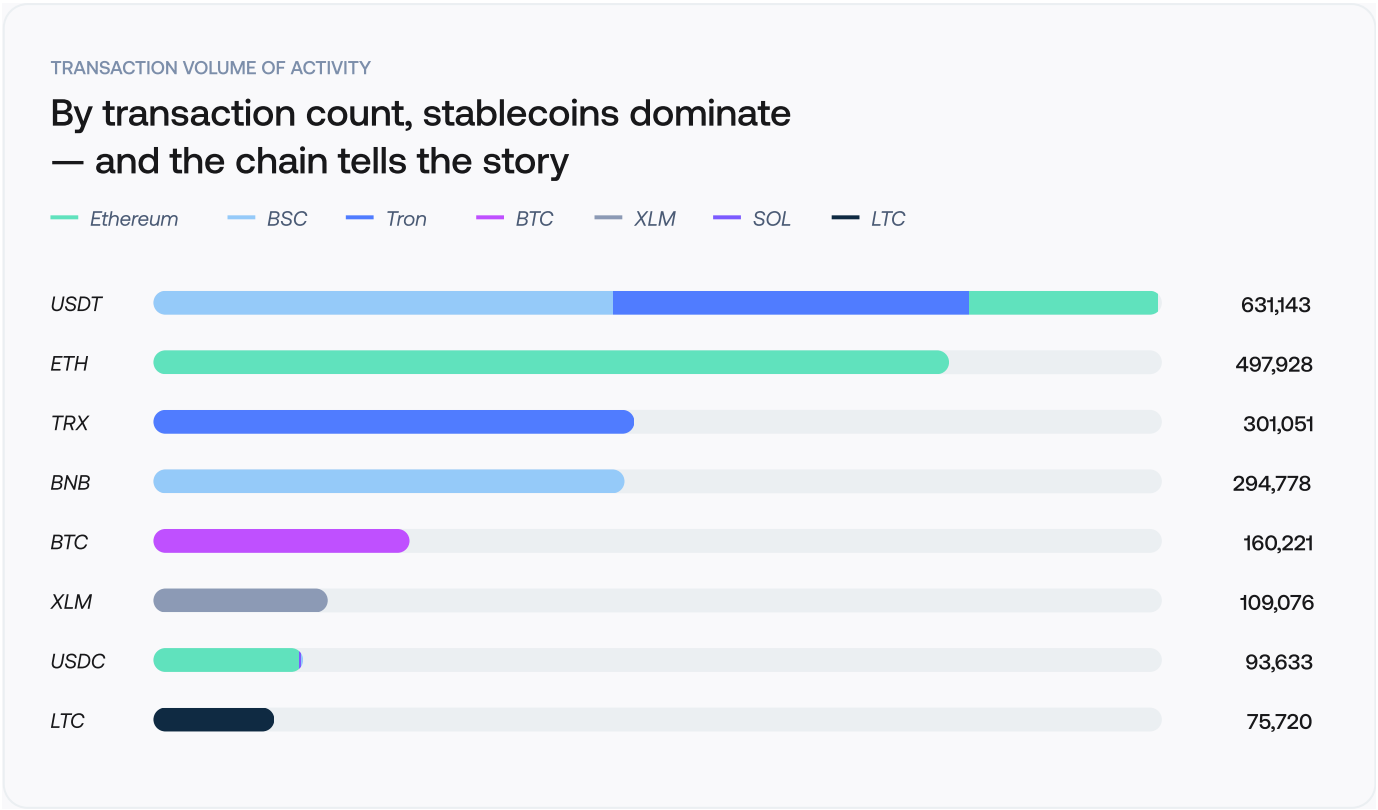
- BTC: 39.2% of volume ($3.13B) across just 160,221 transactions — large-value, wholesale settlement rather than routine activity.
- Stablecoins: 36.1% of volume ($2.88B) across 737,735 transactions — frequent, lower-value customer payments and cross-border settlement.
- ETH: 17.3% of volume across 497,928 transactions, consistent with customer-facing deposits and withdrawals.
- TRX, XLM, and LTC: disproportionately high transaction counts relative to volume, consistent with low-cost, frequent-transfer rails.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Overall, the token distribution indicates that nested services support several distinct transaction functions. BTC is primarily associated with high-value liquidity and wholesale settlement, stablecoins support price-stable payments and cross-border operational flows, while ETH and lower-cost networks facilitate frequent customer-facing transactions. This demonstrates that nested services operate across both wholesale and retail activity, with token choice shaped by transaction size, cost, stability, and settlement requirements.

Transaction count vs. volume

USDT leads with 631,143 transactions, (27.7%), then ETH (497,928, 21.9%); BTC drops to fifth (160,221, 7.0%). TRX and native BSC BNB both outrank BTC by count despite under 1% of volume combined. This is consistent with their use as low-fee settlement rails. USDT itself is chain-agnostic (45.6% BSC, 35.5% Tron, 18.7% Ethereum), while USDC is concentrated on Ethereum (97.5%), suggesting more conservative routing among the services that favor it.

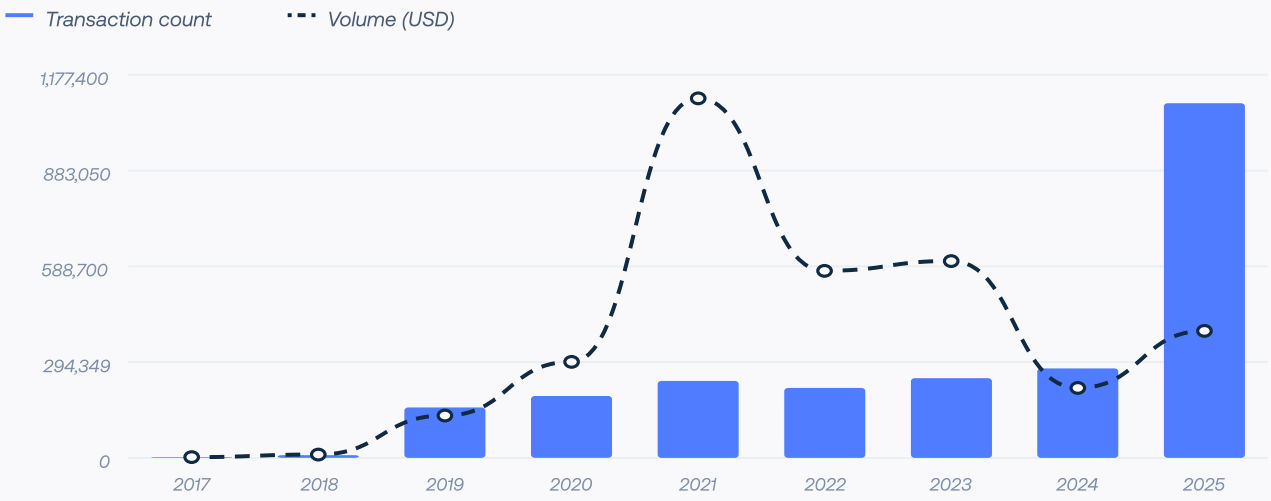


Above: Nested service transaction count by token (SUEX excluded)

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

ACTIVITY VS VALUE

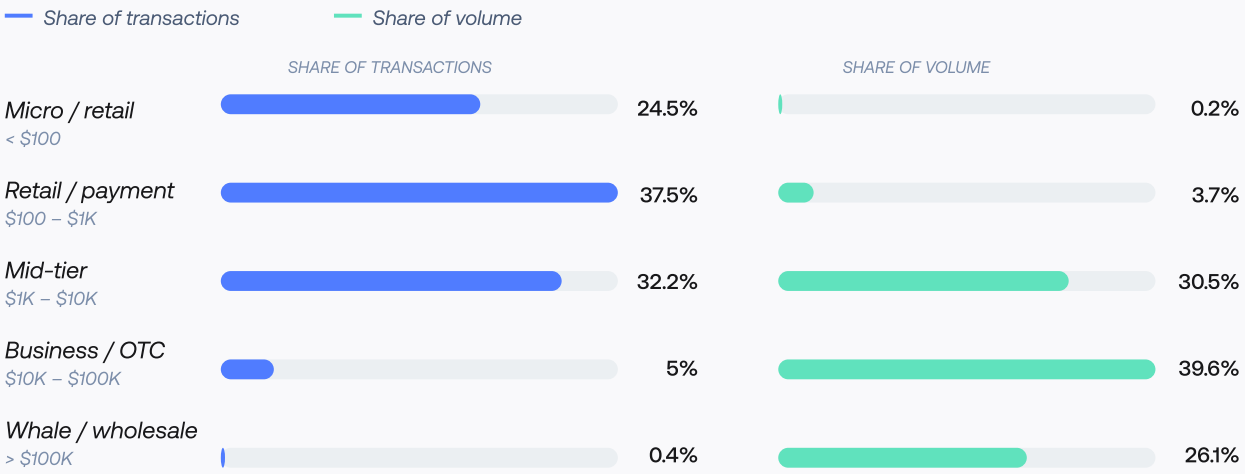
Transaction count is surging even as dollar volume cools



Count and volume have diverged sharply since 2021: volume peaked that year at $2.64B (236,558 transactions, avg. $11,146), while count peaked in 2025 at 1,090,185 transactions (over four times the 2021 count) on just $941M of volume (avg. $863, a 90%+ drop in transaction size). Nested activity hasn't disappeared; more of it is now many small transfers rather than fewer large ones. **Why this matters:** volume-only monitoring misses this shift entirely.

USER TRANSACTION PROFILES

Retail dominates by count: a handful of whales move the value



Above: User transaction profiles: retail dominates by count, whales move the value

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

User transaction profiles by size

Transactions under $1,000 make up 61.9% of count but only 3.9% of volume (retail/payment usage); transactions above $10,000 are just 5.4% of count but 65.6% of volume (wholesale, OTC, and cash-desk activity — Section 5). The mid-tier ($1K–$10K) is roughly proportional at 32.2% of count and 30.5% of volume. Nested infrastructure serves genuinely distinct populations — wholesale and retail — through the very same host accounts, equally invisible to exchange-level monitoring.

Top nested entities by volume

NS-01 and NS-02, both legitimate instant-swap services, together account for over two-thirds of identified volume (excludes SUEX's historical case, see Section 5):

RANK	ENTITY	REGION	HOST	VOLUME
1	NS-01	Global	Tier 1 Global Exchange (Host A)	$2.84B
2	NS-02	Global	Host A, Host D	$2.64B
3	NS-03	MENA	Host A	$371.3M
4	NS-20	Europe	Host A	$237.5M
5	NS-21	Europe	Host A	$175.9M
6	NS-23	Africa	Host N	$135.2M
7	NS-26	Asia	Host O	$118.2M
8	NS-25	Asia	Host P	$111.7M
9	NS-22	Europe	Host F, US	$98.8M
10	NS-24	Africa	Host A	$96.0M

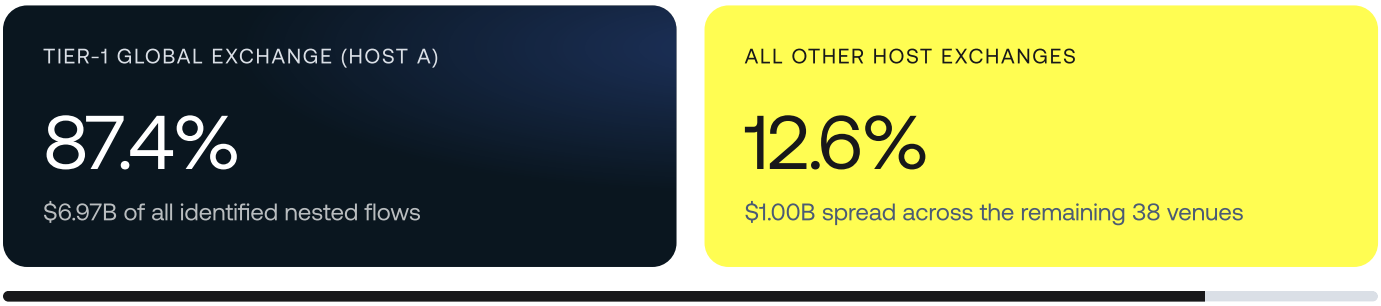
Above: *Top ten nested entities by traced volume, region, and host exchange. Source: Crystal Intelligence*

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

The scale of NS-01 and NS-02 establishes what “normal” nested activity looks like on a major exchange — which is exactly why high-risk or sanctioned operators can blend into that broader population. Effective monitoring requires distinguishing individual entities, not treating all nested activity as one risk category.

Host exchange concentration

Tier-1 Global Exchange (Host A) alone hosts $6.97B, or 87.4% of all identified flows — meaning detection and monitoring improvements at a small number of large exchanges can have an outsized impact on industry-wide AML controls.



Host concentration: Tier-1 Global Exchange (Host A) hosts 87.4% of nested volume. Source: Crystal Intelligence

Multi-host entities

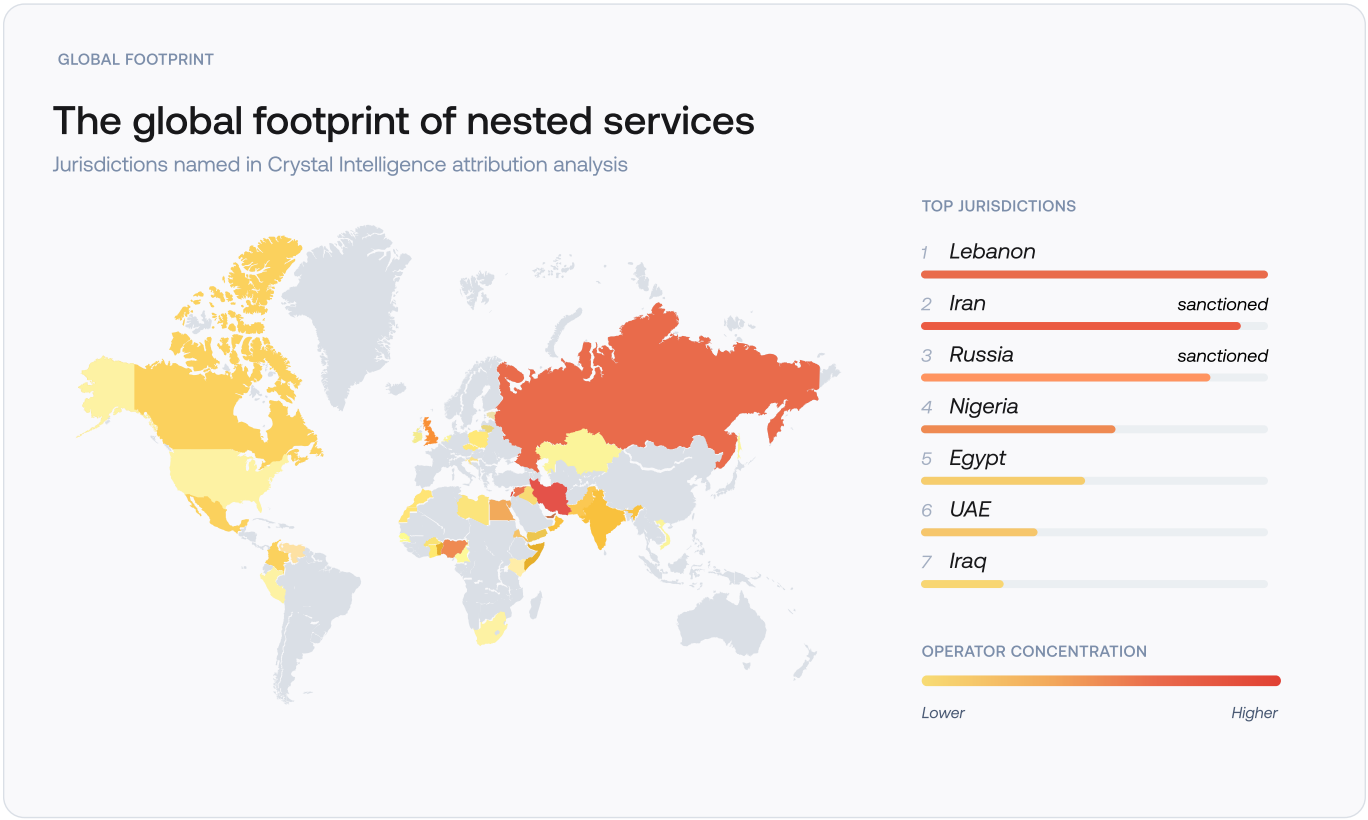
Several entities route through more than one host simultaneously — this can reflect deliberate obfuscation, operational redundancy, or simply large instant-swap services seeking best execution. For example: NS-02 (Host A + Host D), NS-07 (Host A + Regional Exchange, Host I), NS-18 (Host D + Regional Exchange, Host L), and NS-28 (Regional Exchange, Host M + Host A).

Compliance implication: no single exchange holds the full picture for any of these relationships — cross-exchange information sharing or centralized monitoring is essential for a complete risk assessment.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Geographic concentration

Nested services are not uniformly distributed geographically. Crystal Intelligence's attribution analysis identifies seven regional clusters with distinct risk profiles, dominant tokens, and host preferences, based on on-chain indicators, domain registrations, operational intelligence, and direct interaction data.



Above: *Global footprint of nested services*

Geographic risk concentration

The two critical-risk regions, Iran and CIS/Russia, together account for approximately $345M (Iran: $239M; CIS/Russia: $106M), both routing substantially through a small number of major exchanges.

Why this matters: Tier-2 Global Exchange (Host B) for Iran-attributed flows and Tier-1 Global Exchange (Host A) for CIS/Russia-attributed entities host nearly all of this critical-risk volume — targeted monitoring at just these two venues would cover almost the entire sanctions-relevant geographic footprint identified here.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

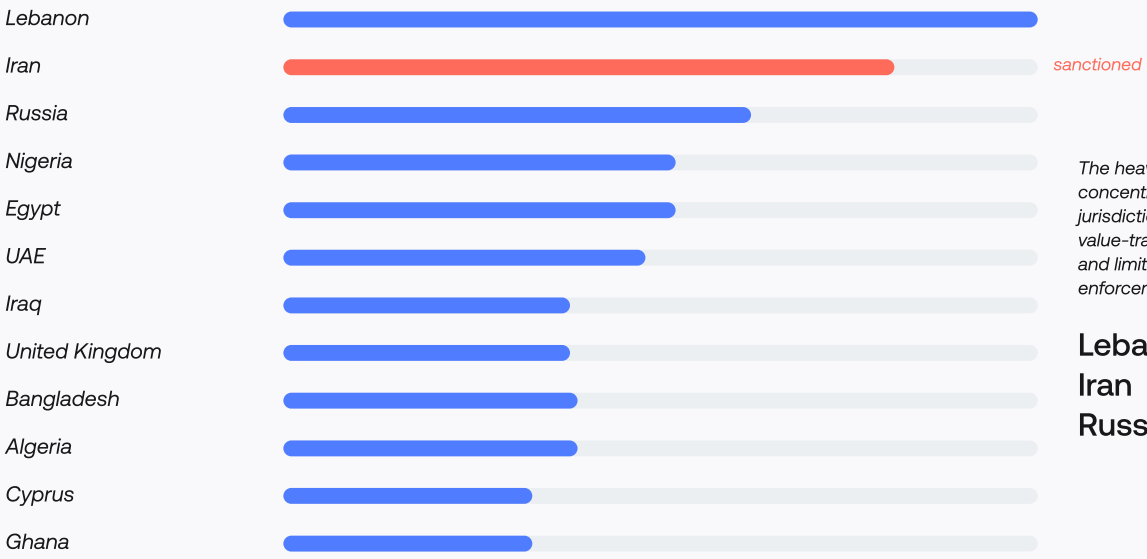
CLUSTER	ENTITIES	HOST(S)	RISK
Iran Sanctions	NS-04 through NS-19 (17 entities, full breakdown below)	Host A, Host B, Host D	Critical
CIS / Russia	NS-28, NS-31	Regional Exchange (Host Q), Host A	Critical
Sub-Saharan Africa	NS-23, NS-24	African-Based Exchange (Host N), Host A	High
MENA	NS-27, NS-32	Host A, Regional Exchange (Host P)	High
South / Southeast Asia	NS-25, NS-26, NS-33	EU Regional Exchange (Host O), Regional Exchange (Host R, CIS-facing)	Medium
Western Europe	NS-20, NS-21, NS-22	Host A, Tier-2 Global Exchange (Host F, US)	Low to medium
LATAM	NS-29, NS-30, NS-34	Host A, Host D	Low

Above: Regional risk overview: seven clusters by risk profile. Source: Crystal Intelligence

GEOGRAPHIC SPREAD

Operators span 60+ countries — concentrated in MENA, CIS & West Africa

The heaviest concentrations sit in jurisdictions with informal value-transfer corridors and limited KYC enforcement.



The heaviest concentrations sit in jurisdictions with informal value-transfer corridors and limited KYC enforcement

Lebanon
Iran
Russia

Above: Geographic spread of nested operators

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

European nested services

NS-20 is the fourth-largest individual entity in the entire dataset — larger than every Iran-cluster entity except NS-04. Three European entities were identified, all routed through global-tier hosts:

ENTITY	VOLUME	HOST(S)
NS-20	$237.5M	Host A
NS-21	$175.9M	Host A
NS-22	$98.8M	Host F (US)

Iran-attributed nested services

The 17 entities in the Iran cluster:

ENTITY	VOLUME	HOST(S)	STATUS
NS-04	$91.8M	Host A	Dormant 2018-2021, cluster leader
NS-05	$55.8M	Host B	Active, retail payment gateway
NS-06	$39.1M	Host B	Active, card-linked (Case study 2)
NS-07	$16.3M	Host A + Host I	Active, mid-tier
NS-09	$11.7M	Host A	Dormant
NS-10	$7.7M	Host A + Host B (dual)	Active
NS-11	$6M	Host A	—
NS-08	$5.6M	Host D	Dormant
NS-18	$1.9M	Host D + Host L	Active
NS-12, NS-13, NS-14	—	Host B	Active, grouped with NS-05/NS-06
NS-15, NS-16, NS-17, NS-19	—	Host D	Active, grouped with NS-08/NS-18

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Iran-facing nested services account for approximately $239M across these 17 entities, led by NS-04 (historical) and NS-05 (currently active), routed primarily through Tier-1 Global Exchange (Host A) and Tier-2 Global Exchange (Host B). These services present elevated sanctions exposure under the Iran Transactions and Sanctions Regulations (ITSR) and Executive Order 13599; NS-04 is Iran's largest domestic cryptocurrency exchange.

Iran cluster entity overview

NS-04: the dormant liquidity gateway

Iran's largest domestic crypto exchange and the highest-volume entity in the cluster. Activity concentrated between 2018 and 2021, after which its relationship with Tier-1 Global Exchange (Host A) went dormant. The low transaction count relative to volume reflects its role as a primary liquidity gateway rather than a retail-facing service.

NS-05: the active payment gateway

The largest active entity in the cluster, with activity spanning October 2023 through December 2025 and continuing as of the most recent data. Operates as a payment gateway for Iranian merchants and consumers, providing rial/crypto conversion. Its high transaction count and moderate average size indicate a retail-facing, high-frequency operation.

OFAC SANCTIONS WARNING: IRAN-ATTRIBUTED ENTITIES

All 17 entities in the Iran cluster are subject to OFAC primary sanctions under the Iran Transactions and Sanctions Regulations (ITSRs). Any US person or US-nexus entity that processes transactions for these services, or facilitates their access to financial infrastructure, may be in violation of US sanctions law. Host exchanges with US nexus (including Binance US, Kraken, and Coinbase) should treat Iran-attributed nested service detection as a Tier 1 compliance priority.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Two exchanges anchor the Iran cluster

Cluster volume concentrates on two hosts:

- Tier-1 Global Exchange (Host A) carries approximately $133M (54%) across NS-04, NS-07, NS-09, NS-10 (dual-host), and NS-11;
- Tier-2 Global Exchange (Host B) carries approximately $103M (43%) across NS-05, NS-06, NS-10 (dual-host), NS-12, NS-13, and NS-14;
- A third host, Tier-2 Global Exchange (Host D), plus two smaller regional exchanges (Host J and Host K, Turkey), account for the remaining volume, bringing the total number of host exchanges identified in the Iran cluster to seven.

Why this matters:

Two entities, NS-04 (historical) and NS-05 (currently active), account for the majority of the Iran cluster volume. A handful of specific operators drive nearly all of this cluster's sanctions exposure, not a diffuse universe of small actors.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 5

What does the problem look like?

The following case studies illustrate how nested infrastructure is used across both legitimate and illicit contexts. The underlying technical model is the same regardless of whether the nested entity is a licensed business, an unregulated exchange, or a sanctioned actor what differs is the visibility of the relationship to the host, and the effectiveness of downstream compliance controls.

Case study 1: MENA High-net-worth crypto cash desks (NS-03)

NS-03 operated through Tier-1 Global Exchange (Host A), processing $371,307,600 across 11,153 transactions—the third-largest entity in the dataset by volume. It operated without a license from its jurisdiction's designated virtual asset regulator and did not apply meaningful KYC controls to its underlying customers.

Its average transaction value of approximately $33,300 is consistent with a high-value OTC operation serving high-net-worth individuals, brokers, and businesses rather than a retail-facing service. Cash desks of this type, often imposing minimum transactions of $5,000 or more, are common across major OTC hubs and allow customers to convert cash and cryptocurrency with limited or no identity verification.

The combination of unlicensed status, no-KYC customer access, high transaction values, and cash-based OTC activity materially increases the risk of the relationship. Host A holds KYC information only for NS-03 as its direct customer; it has no visibility into the identity, source of funds, or beneficial ownership of the customers transacting through the service.

Consequently, those customers can indirectly access Host A's regulated infrastructure through a separate and substantially weaker compliance framework.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Case study 2: SUEX — a historical precedent for sanctions enforcement

SUEX OTC, S.R.O., a Czech Republic-registered exchange, processed $1.86B in nested volume — ranking third by volume among identified entities — primarily through Tier-1 Global Exchange (Host A) and Tier-2 Global Exchange (Host C), before becoming the first virtual currency exchange OFAC ever sanctioned.

On September 21, 2021, OFAC designated SUEX a Specially Designated National under Executive Order 13694, citing its facilitation of transactions tied to at least eight ransomware variants, with over 40% of its known transaction history linked to illicit actors.

Its regulated hosts wound the relationship down immediately after designation, and its nested activity ceased.

SUEX's $1.86B is excluded from this report's aggregate figures (total volume, host concentration, token distribution, geographic totals) to avoid overstating current, live exposure — it represents roughly 18% of what the aggregate dataset would otherwise total.

It remains a standalone case study for two reasons: it shows the scale a nested service can reach before intervention, and its designation-to-cessation outcome is the clearest completed enforcement cycle in this dataset, a useful reference point against the still-active cases elsewhere in this report (NS-06, NS-03, NS-27, and the Iran-attributed entities in Section 4).

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

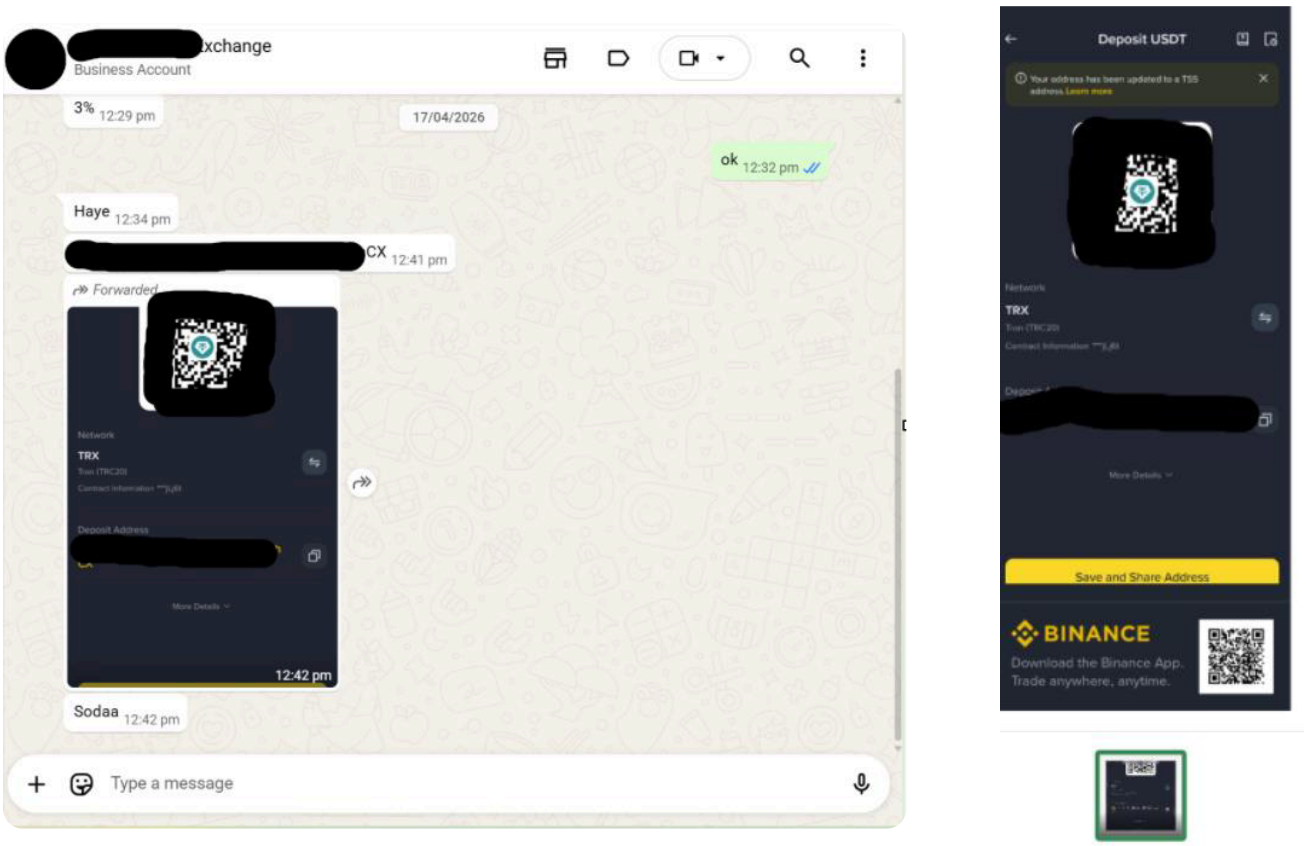
SECTION 6

Detecting nested services

Crystal Intelligence uses a multi-layered methodology to identify and confirm nested-service relationships. No single indicator is sufficient on its own; attribution requires convergence of multiple evidence streams.

Primary method: direct interaction testing

Analysts interact with candidate services as simulated customers, initiating test transactions and tracing the resulting on-chain activity to determine the deposit address's ultimate attribution. When funds route to a hot wallet attributable to a known exchange, the nested relationship is confirmed — this is the gold-standard, primary basis for high-confidence attribution.

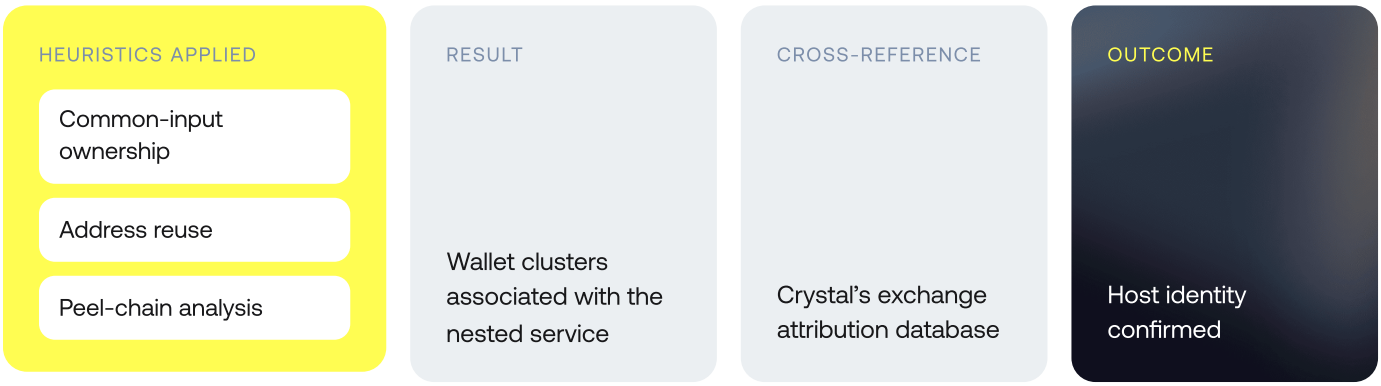


This method is the primary basis for high-confidence attribution. When the deposit address presented by the nested service resolves to a known exchange cluster, the nested relationship is considered confirmed. Source: Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Confirmatory method: on-chain cluster analysis

Used to confirm and extend direct-interaction findings: common-input ownership heuristics, address-reuse patterns, and peel-chain analysis identify wallet clusters associated with the nested service, which are then cross-referenced against Crystal's exchange attribution database to confirm host identity.



Above: On-chain cluster analysis confirming a host relationship. Source: Crystal Intelligence

On-chain behavioral signals

Six recurring signals:

01 Consistent fund-forwarding to a known hot wallet	02 Automated sweeping within 30–60 minutes of receipt
03 Threshold-triggered batch sweeps	04 Aggregation of multiple deposit addresses into one wallet
05 Withdrawals originating from the host's hot wallet rather than a self-custodied address	06 Near-zero running balances

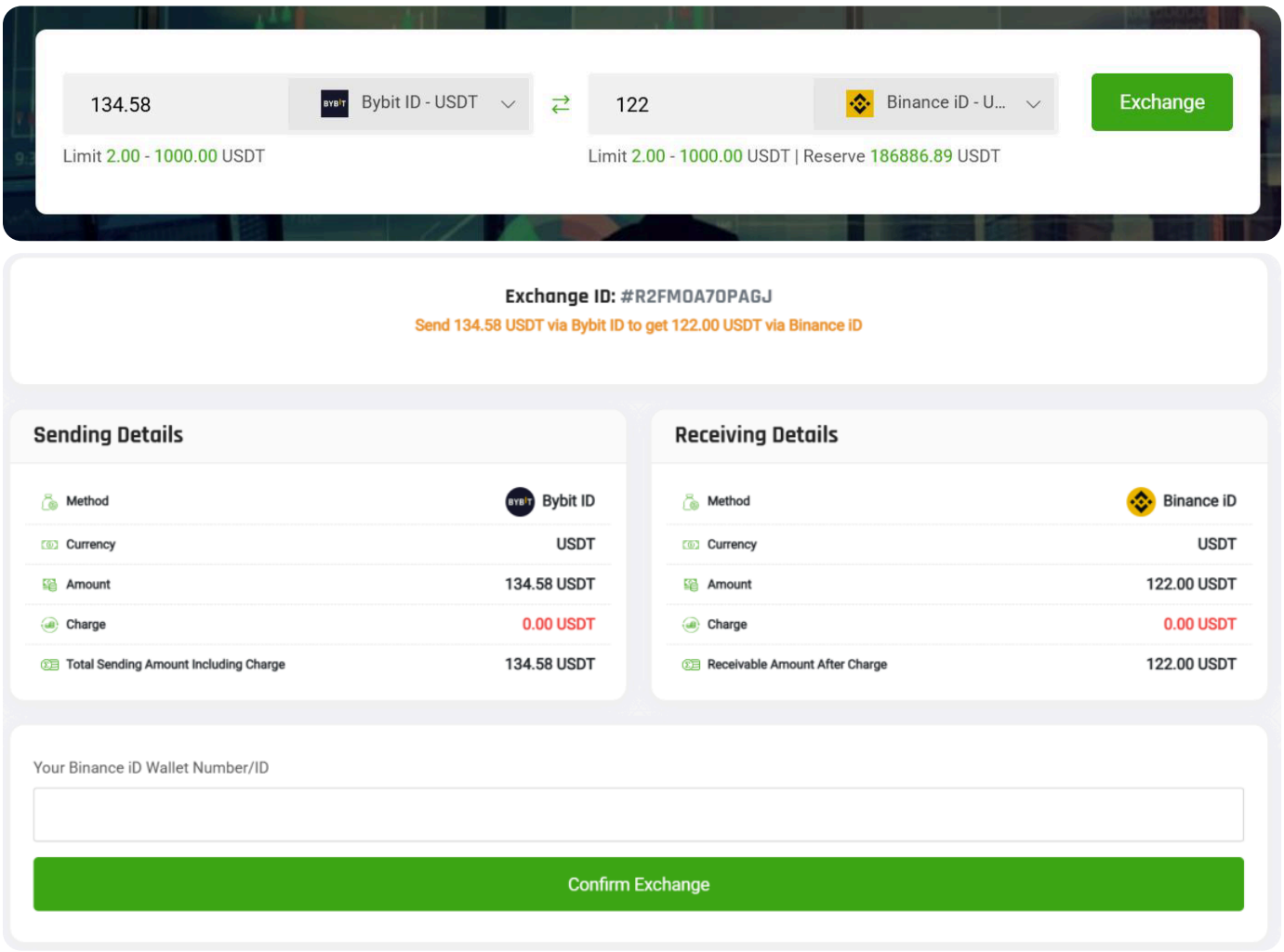
Above: The six recurring on-chain behavioral signals. Source: Crystal Intelligence

No single signal confirms a relationship alone, but convergence across several is a strong indicator.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Using AI agents to spot nested services

This detection methodology is well-suited to AI agent automation — worth evaluating now, not treating as a future concern. An agent can handle much of the first-pass work: matching deposit addresses against known exchange clusters in real-time, flagging behavioral patterns typical of nested activity, and scanning public documentation for red flags such as missing custody statements. It doesn't replace direct interaction testing or on-chain cluster analysis as confirmatory methods — used as a triage layer, it lets compliance teams prioritize which accounts warrant closer review, at a scale manual monitoring can't match.



Above: An illustration of how nested services can indicate that they operate on top of another provider's infrastructure. For example, the service shown supports sending payments internally via Binance ID and receiving payments via Bybit ID. This is a strong indicator that the service is nested and relies on a third-party infrastructure rather than operating its own independent network. Source: Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Attribution confidence levels

Findings are graded on a four-level scale: Highest confidence (deposit-address match to a known cluster plus an interface/branding match) is auto-confirmed. High confidence (confirmed on-chain sweep behavior to a known hot wallet) is flagged for analyst review. Moderate confidence (behavioral pattern match, host not yet identified) is queued for manual investigation. Supporting-only signals (OSINT, no on-chain confirmation) are logged but not used to attribute a relationship on their own.

LEVEL	EVIDENCE	ACTION
Highest confidence	Deposit-address match to a known cluster plus an interface/branding match	Auto-confirmed
High confidence	Confirmed on-chain sweep behavior to a known hot wallet	Flagged for analyst review
Moderate confidence	Behavioral pattern match, host not yet identified	Queued for manual investigation
Supporting only	OSINT, no on-chain confirmation	Logged, not used to attribute a relationship alone

Above: The four-level attribution confidence scale. Source: Crystal Intelligence

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

SECTION 7

Closing the blind spot

Five primary risk areas

Closing the blind spot means controlling for five risk areas:

	RISK AREA	WHAT HAPPENS	HOW IT IS ADDRESSED
01	Attribution gap	On-chain activity appears to originate from the host, masking the true nested operator.	Addressed by entity-level attribution, not exchange-level counterparty checks alone.
02	KYC/AML gap	Cash-desk and OTC models impose no verification.	Addressed by cross-referencing no-KYC claims against on-chain attribution and treating zero-KYC models as high-risk.
03	Sanctions evasion	Nested services in sanctioned jurisdictions gain indirect access to major exchanges.	Addressed through host-level exposure analysis and enhanced due diligence on sanctioned-jurisdiction deposit pools.
04	Regulatory arbitrage	Nested services operate with no clear legal entity or licensing.	Addressed by requiring explicit licensing documentation as a condition of onboarding.
05	Layered accountability	Neither host nor nested service has full visibility into the relationship.	Addressed through combined on- and off-chain analysis and contractual audit rights reaching nested-service user data.

Above: The five risk areas nested services create, and the control for each. Source: Crystal Intelligence

Recommendations by audience

For host exchanges (Binance, HTX, CoinEx, KuCoin, others)

- Implement dedicated nested service detection programs using blockchain analytics providers capable of direct interaction testing and on-chain attribution at the entity level.
- Apply enhanced due diligence to accounts exhibiting nested service behavioral signatures: high volume, low transaction count, consistent counterparty patterns, intermediary wallet hops.
- Establish a formal nested service disclosure obligation: accounts operating as nested services must self-declare and provide sub-customer KYC information or face termination.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

For regulators and FATF

- Issue specific FATF guidance on nested service typologies and the obligations of host exchanges with respect to nested service customers.
- Require exchanges to conduct periodic nested service audits and report findings to financial intelligence units.
- Consider nested service hosting as a Material Risk Factor in exchange licensing assessments.

For correspondent banks and payment processors

- Where cryptocurrency exchange clients are held, assess whether those exchanges have adequate nested service controls before extending correspondent relationships.
- Require exchanges to provide nested service exposure data as part of annual correspondent banking due diligence questionnaires.

About Crystal Intelligence

Crystal Intelligence provides blockchain intelligence solutions for financial institutions, law enforcement agencies, virtual asset service providers, and regulators. The company's platform enables organizations to detect crypto fraud, trace digital funds across 330+ blockchains, and maintain regulatory compliance. With over 110,000 attributed entities and 30 million risky transfers flagged, Crystal Intelligence helps organizations uncover on- and off-chain risk in crypto transactions. The company is ISO 27001 and GDPR compliant. For more information, visit crystalintelligence.com.
See what is hiding in your transaction flows. Ready to close the blind spot? Get Crystal.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.

Appendix

Scope

Sample scope	nested service entities analyzed in this report were drawn from the Crystal Intelligence attribution database. Entities were selected based on confirmed or high-confidence attribution: direct platform interaction confirming a host exchange dependency, or on-chain behavioral analysis demonstrating fund forwarding, automated sweeping, or aggregation patterns consistent with nested operation.
Address attribution	2,052 wallet addresses have been attributed to the identified nested service entities in this dataset, following Crystal Intelligence's dual tag/label model (tagging the nested service, labeling the controlling host). Volume and transaction figures are derived from on-chain data at these attributed addresses.
Time period	January 2017 through December 2025.
Chains covered	Bitcoin (BTC), Ethereum (ETH/ERC-20), Tron (TRX/TRC-20), Litecoin, Stellar, and other chains represented in the attributed address dataset (chains under 0.1% of total volume are aggregated, not broken out).
Volume methodology	the absolute sum of inflows and outflows at attributed nested service addresses, in USD at average monthly price at time of transaction — direct transfers at attributed addresses, not aggregate exchange-to-exchange settlement volume.
Limitations	this dataset represents only nested services identified by Crystal Intelligence; the true population is likely larger. XRP-based activity was excluded because XRP commonly uses shared deposit addresses with Destination Tags, making nested service activity difficult to reliably attribute at the address level. The Iran cluster's headline entity count is 17; 16 are individually profiled in this report (NS-04 through NS-19) with figures currently available — the 17th is included in the cluster totals pending a fully broken-out figure.
Exact total transaction volume	$7.97B, rounded to $8B throughout this report for readability. All aggregate figures in this Appendix use the precise, unrounded value.

Copyright © 2026 Crystal Intelligence B.V. All rights reserved.



© 2026 Crystal Intelligence. All rights reserved.

This report is intended for informational purposes only. The data provided herein is based on information publicly available and analysis conducted by Crystal Intelligence. Crystal Intelligence accepts no liability for actions taken based on this information. Readers are advised to perform independent verification and seek professional advice where necessary.