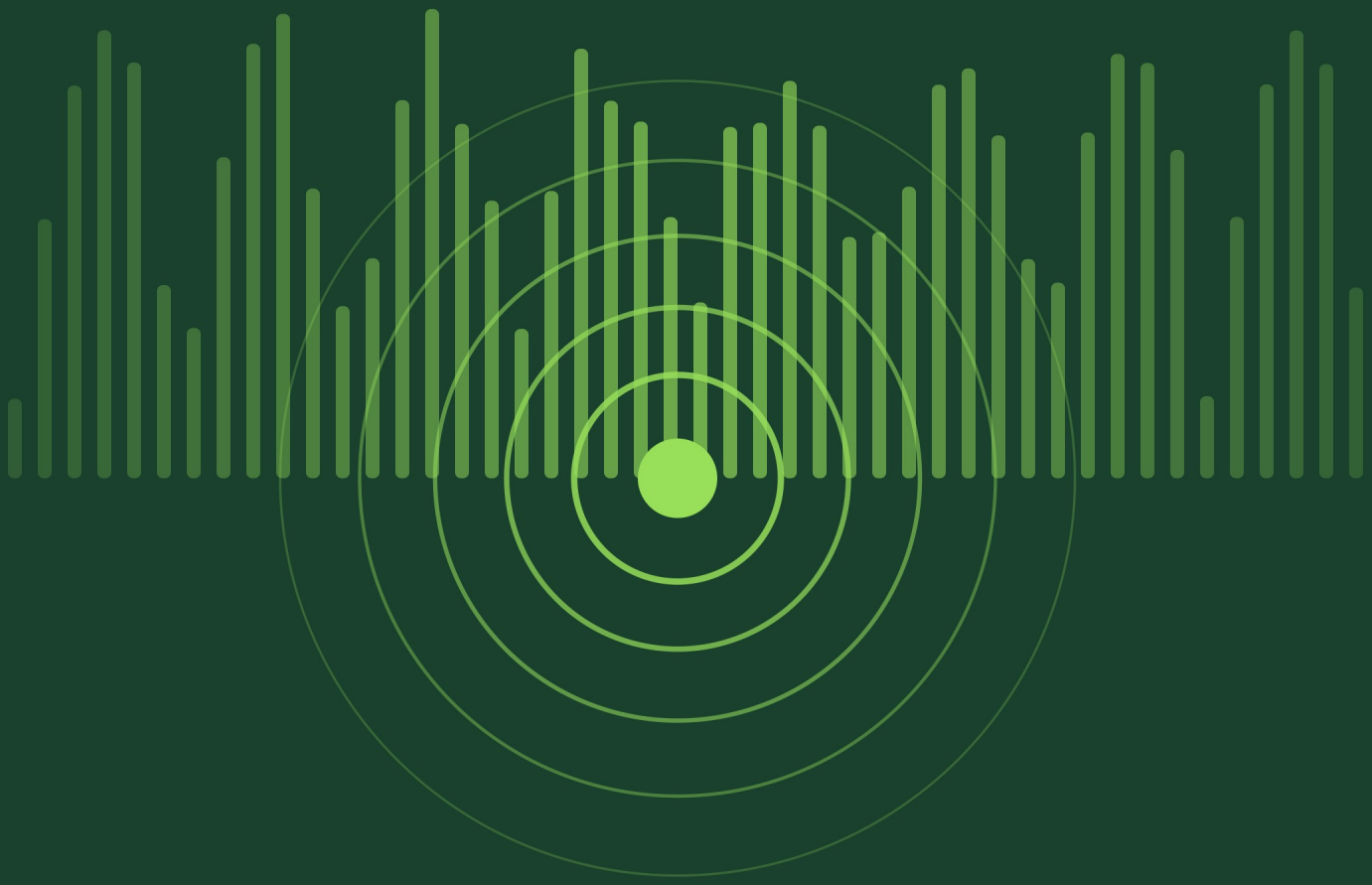
coingecko API

In partnership with DIGITAL ASSET RESEARCH



Breadth Meets Depth

Assessing Crypto Exchange Risk: Lessons From FTX to the Binance Hack

November 2026

Need exchange data? coingecko.com/api

Key Takeaways

On 10 November 2026, CoinGecko and Digital Asset Research hosted an invite-only webinar for institutional participants on how to assess the risk of trading with, and holding assets on, centralised crypto exchanges. This report draws on that discussion, CoinGecko data and DAR's diligence experience.

Exchange risk is counterparty credit risk

Centralised exchanges hold an estimated $250B+ in client assets. Leaving assets on a venue is effectively an unsecured loan to it, and the Binance hack on 29 October 2026, the largest on record at more than $6.3B, shows the scale of what is at stake.

No single score is enough: breadth meets depth

CoinGecko's Trust Score rates 150+ of the 215 exchanges it tracks on liquidity, cybersecurity, regulation, past incidents and proof of reserves. It focuses on breadth to cover as many exchanges as possible. Institutional diligence of the kind Digital Asset Research (DAR) conducts zooms in with deep due diligence on specific exchanges.

A checklist is where diligence starts, not where it ends

Asking for a SOC report is table stakes. The real signal comes from a critical read of its scope and exceptions, proof of the policies and processes behind it, and interactions with the people who run the exchange.

Reluctance is a red flag

FTX never passed DAR's diligence. It provided preliminary materials, then said it would not provide more and stopped responding. DAR says it identified FTX as an uncreditworthy counterparty roughly 18 months to two years before its collapse.

Plan for a loss, not only for proof of reserves

Proof of reserves shows what a venue holds, not whether it can absorb a loss on the scale of the Binance hack. Assess that ability, and consider removing assets during periods when you are not actively exposed.

Diligence is never one and done

Order books can deteriorate in days. Security posture and regulatory status change. Monitor score changes, news and personnel moves, and re-run deep diligence periodically.

About This Report

From the webinar: Assessing Crypto Exchange Risk: Breadth Meets Depth

Exchanges remain an integral part of the digital asset ecosystem. Whether an institution trades directly, routes client orders or holds collateral on a venue, at some point it will interact with a centralized exchange, and that relationship carries real counterparty risk.

The session brought together two complementary perspectives. CoinGecko assesses exchanges programmatically and at scale, across the whole market. Digital Asset Research goes deep, running institutional-grade diligence on individual exchanges and custodians for its clients.

This report sets out what each approach can and cannot see, adds supporting CoinGecko data, and closes with a practical framework. An appendix lists the CoinGecko API endpoints you can call to run your own screen.

Quotes have been lightly edited for clarity and length. Figures are as cited during the session or as of the dates shown. This report is for information only and is not investment advice.

The speakers



Zhong Yang Chan, Head of Research, CoinGecko

Zhong leads the team behind CoinGecko's Exchange Trust Score, which rates the exchanges CoinGecko tracks and was rebuilt from the ground up in 2026 for an increasingly institutional market.



Doug Schwenk, CEO, Digital Asset Research

Doug leads DAR, which has evaluated exchanges since 2017–18 for institutional clients.



Adam Capon, COO, Digital Asset Research

Adam runs DAR's diligence engagements. He brings an operational background in custody and traditional finance to the vetting of exchanges and custodians for institutional clients.

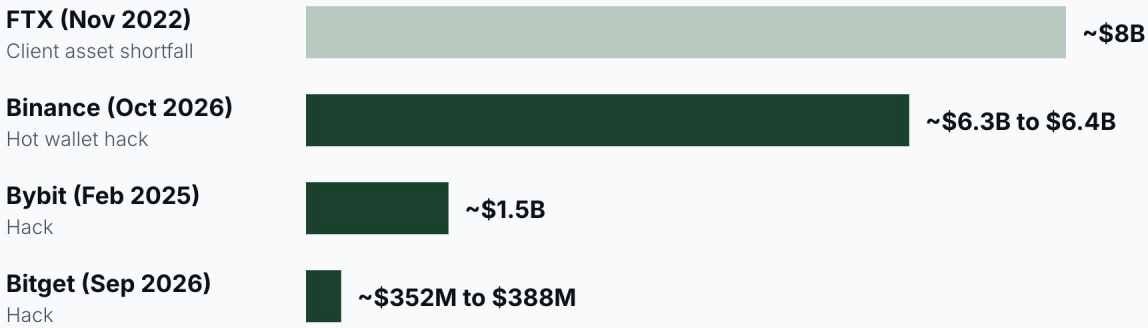
I. How Exchanges Fail

Exchanges hold the assets, so exchanges are the target

Exchanges fail their clients in two ways: assets are stolen from outside, or misused or misplaced inside. Both have now happened at record scale. On 29 October 2026, attackers drained more than $6.3B from Binance's hot wallets, the largest crypto theft on record and more than four times the previous record, Bybit's ~$1.5B hack in February 2025 (Exhibit 1). The FBI attributed the attack to North Korea[1].

The hacks are not isolated. While Binance alone accounted for around three quarters of all crypto hack losses recorded in 2026 (Exhibit 2), it followed a string of incidents, including Bitget's recent hacking incident where an estimated $352M to $388M were lost in September 2026[2]. Exchanges are targets because of what they hold, and the attackers now include state-sponsored groups.

Exhibit 1: Largest centralised exchange losses (USD)



Source: FTX shortfall per bankruptcy proceedings as cited in the webinar; Binance estimates from Binance (~$6.34B), Chainalysis (~$6.4B) and Elliptic ($6.43B); Bybit and Bitget per public reporting. Figures vary by valuation method.

Exhibit 2: Binance's share of all recorded crypto hack losses in 2026



Total: ~$8.78B stolen across 328 recorded incidents, year to date

Source: DefiLlama hack database, as of 4 November 2026.

[1] https://www.fbi.gov/investigate/cyber/alerts/2026/north-korea-responsible-for-6-billion-binance-attack
[2] https://www.ft.com/content/14aed3cb-492e-45c1-b217-869790b6130d?syn-25a6b1a6=1

The second failure mode is internal. When FTX's accounts were reconciled, $8B of client assets were missing, having been diverted to its affiliated trading firm, Alameda Research[3]. Liquidity metrics alone would not have revealed either risk.

The Binance hack also changes what an institution should ask. Proof of reserves shows how much client assets were being held by the exchange, not whether a counterparty can withstand an event of this size. DAR's advice is to assess that ability directly and, even when trading with an exchange, to consider removing assets during periods when you are not actively exposed.

“When you're an institution looking to trade on a crypto exchange, you've probably asked yourself how safe or trustworthy they may be. The answer is not as clear as it may seem.”

Zhong Yang Chan, Head of Research, CoinGecko

[3] https://www.wsj.com/articles/ftx-says-8-9-billion-in-customer-funds-are-missing-c232f684

II. What a Broad Score Sees

CoinGecko's Exchange Trust Score, first introduced in 2019

A broad score answers the first question: where to look. CoinGecko launched its Exchange Trust Score in 2019, when the market was broadly retail-dominated and users traded directly on exchange front ends (Exhibit 3). The early versions compared reported trading volume with web traffic to flag venues reporting volume far out of line with real web activity, and introduced a normalized trading volume to show what was actually happening on each exchange.

A few months later the score moved to a 1 to 10 scale, and CoinGecko began ranking exchanges by Trust Score rather than by reported volume, and this practice has persisted even today. Components were added as the market matured: cybersecurity, team presence and past incidents, and proof of reserves.

The trust score calculation method is algorithmic by design. CoinGecko aims to cover the entire market, from global to local exchanges, and manual due diligence is impossible at scale.

In May 2026, CoinGecko rebuilt the score from scratch with the Basilisk update, as crypto trading activity evolved. Trading today runs largely through APIs and mobile apps, institutions are active, and a major global exchange typically runs OTC and prime brokerage desks alongside its spot order book. The way exchanges are assessed needed to change with them.

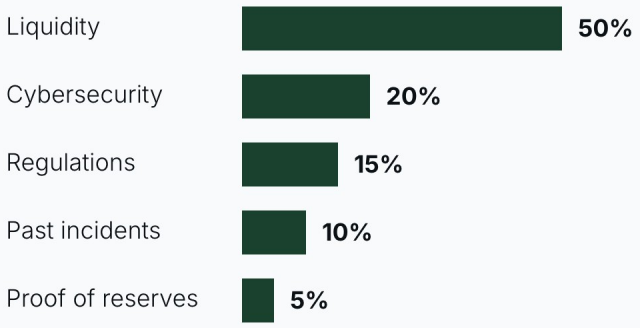
Exhibit 3: Evolution of the CoinGecko Exchange Trust Score

Date	Change
May 2019	Launched to detect and filter out wash trading; normalised trading volume introduced
Sep 2019	Exchanges graded on a 1 to 10 scale and ranked by Trust Score instead of pure volume
Jul 2020	Cybersecurity component added, in collaboration with Hacken
Nov 2020	Team presence and past incidents added for greater transparency
Jan 2023	Proof of reserves added post-FTX, with DefiLlama
May 2026	Basilisk: methodology rebuilt from scratch for an evolving market

Source: CoinGecko methodology.

Basilisk: What the Trust Score Measures

Exhibit 4: Trust Score components and weights



Source: CoinGecko Trust Score methodology (Basilisk, May 2026). Final scores TS1 to TS10 are assigned on a curve after weighted raw scores are combined.

Liquidity is half the score

CoinGecko snapshots exchange order books regularly, assessing depth from the top of the book out to 2% from the last traded price (Exhibit 4). Web traffic is no longer used as a proxy, since some venues are almost entirely institutional and generate significant volume with little web traffic.

A reference set of around 50 coins common to most major exchanges, together with a group of trusted benchmark exchanges, is used to build liquidity thresholds and ratios. Every exchange is compared against them, across every evaluated trading pair: a few clean pairs are not enough. Exchanges need to demonstrate healthy orderbooks across all coins to score well.

> "Some exchanges report a lot of volume and very low order book liquidity. That's bad. But there are also exchanges that report a lot of liquidity and not a lot of volume. That doesn't make sense to us either."

Zhong Yang Chan, Head of Research, CoinGecko

Grading on a curve

The biggest change in Basilisk is that final scores are graded on a curve, benchmarking each exchange against market leaders rather than against fixed thresholds. With an absolute score, more and more exchanges reach the top end as the market matures, and the score says less about their relative quality. A curve keeps the ranking relevant as standards are raised.

The other half

Cybersecurity is assessed by CORE3, a risk intelligence platform powered by Hacken, covering server and user security, bug bounties, insurance funds, certifications and penetration testing. **Regulation** checks each claimed licence against the official register and tiers regulators by strictness and enforcement track record; only the strongest verified spot credential counts. **Past incidents** and **proof of reserves**, verified via DefiLlama and then by CoinGecko, make up the rest.

Reading the Signals

The Exchange Trust Score is generally updated weekly, reducing the noise from minor liquidity shifts while still capturing larger movements. Cybersecurity and regulation inputs update as changes happen, with cybersecurity scores refreshing within 48 hours of CORE3 verification. CoinGecko's exchange pages show the breakdown of each score, so when an exchange's overall trust score drops or jumps, a user can see which component moved (Exhibit 5).

Exhibit 5: What Trust Score changes may indicate

Signal	Possible scenarios
Low or sharply falling liquidity score	Possible wash trading or fake volume; traders or market makers retreating, for example after sanctions or a lost market-maker contract
Cybersecurity score changes	A new audit, certification or security finding, or certifications such as a penetration test going out of date
Regulation score changes	A licence granted, expired or lost, for example during the transition to MiCA licensing
Sudden drop in incident score	A security or operational incident; CoinGecko typically posts a public notice
Proof of reserves changes or lapses	A shift in assets held against exchange liabilities

Source: CoinGecko Research, as presented at the webinar.

Red flags in liquidity data

Order book liquidity tends to reflect the state of an exchange quickly. When a major exchange was recently sanctioned, its order book deteriorated over days and weeks, and its Trust Score fell with it. Outside of external factors, there are also unusual observable patterns within orderbooks that are red flags:

- **Repeating trades.** The same trade, at the same size, again and again is almost certainly wash trading.
- **Liquidity parked out of reach.** Some venues stack orders at the edge of the 2% band to game depth metrics while the book near the last traded price is thin. Basilisk now assesses depth at multiple levels.
- **Lopsided books and extreme liquidity ratios.** Most major exchanges now run several market makers, so heavily unbalanced books are rare, unless during times of significant market volatility; volume-to-liquidity ratios of 100 times or more cannot be real.

III. What a Broad Score Cannot See

A programmatic score can only assess what is verifiable: the lit order book, on-chain data and an independent cybersecurity rating. However a sizable chunk of an exchange's real risk can lie elsewhere (Exhibit 6). Flows from OTC and prime brokerage desks do not show in the lit book, and a venue's processes and terms of service can be read, but they do not show whether it actually carries out these processes diligently.

Exhibit 6: What a broad score sees versus what needs deeper diligence

Visible to CoinGecko	Needs deeper diligence
Lit order book depth and trading volume from public APIs, matched with the exchange front end	Flows from OTC and prime brokerage desks
On-chain proof of reserves	Actual off-chain liabilities to customers versus reserves held on-chain
Independent cybersecurity rating	Custody, wallet set-up and withdrawal infrastructure
Spot licences verified on official registers	Compliance processes in practice
Reported hacks and incidents	Balance sheet strength to absorb losses
Public profiles of leadership teams	Final beneficial ownership and board governance

Source: CoinGecko Research.

Nobody can deep dive every exchange

Compared to retail traders, an institution may want to conduct deeper due diligence on an exchange before entering into a relationship, but with so many exchanges out there it's impossible to assess every one in detail. The practical answer is a funnel.

Use a broad score such as CoinGecko's Exchange Trust Score to cut the universe down to a shortlist, for example the ten or fifteen exchanges with a Trust Score of 9 or 10. Then spend diligence time and effort on the handful of venues you will actually consider using, assessed with a specialist such as DAR or by gathering the information yourself.

IV. How Deep Diligence Fills the Gap

Commercial success is not institutional readiness

A shortlist answers where to look. It does not answer whether a venue meets your standards as a counterparty, or how you document that it does. DAR's work rests on one distinction: commercial success and institutional readiness are not necessarily the same thing. Trading volume, liquidity and reputation are surface appearance, and they should be supported by proper controls, governance and risk management.

The work starts with data. DAR receives trade data from hundreds of venues and runs tests to verify that trades represent true economic activity, producing lists of vetted and watch-list exchanges that combine quantitative analysis with qualitative deep dives.

Those deep dives examine three foundations: price quality and market integrity; financial and business risk, including whether a venue can sustain a business through lengthy institutional onboarding; and asset protection and recoverability under market-wide or token-specific stress.

They are organised around four pillars (Exhibit 7). Governance benefits most from an engagement that goes beyond exchanging documents and questionnaires. The technical pillar needs specialist knowledge, because organizations are facing attacks that are increasing in sophistication each day.

> **"Protecting private keys are more akin to physical security than many TradFi organisations have encountered before."**
>
> **Adam Capon**, COO, Digital Asset Research

Exhibit 7: The four pillars of institutional diligence

Pillar	What it covers
Regulatory	Registrations, history and issues, jurisdiction matrix, KYC and AML
Governance	Processes and controls, audits and control reports, vendor risk
Financial	Financial statements, insurance, audits, ability to absorb losses
Technical	Private key security, cybersecurity, custody and exchange controls

Source: Digital Asset Research.

How a Deep Dive Engagement Works

Every engagement starts with why the client is vetting the counterparty. Diligence on an exchange function can differ materially from diligence on the same organisation's custody function, and may rely on different experts inside the target. The process is iterative: documents prompt follow-up requests, findings are tested in calls with subject matter experts and executives, and the report sets a cadence for ongoing monitoring (Exhibit 8).

Exhibit 8: The DAR diligence process

Step	Stage	What happens
1	**Engage**	Understand client profile and intended use; connect with counterparty
2	**Consent to share**	Obtain consent for DAR to share confidential data with the client
3	**Document request**	Issue a tailored document request list
4	**Review materials**	Analyse operational, security, financial, insurance and custody policies
5	**Q&A with SMEs**	Deep-dive calls with subject matter experts and executives
6	**Diligence report**	Synthesise findings; risk assessment based on client profile
7	**Client discussion**	Review findings and risk profile with the client
8	**Follow-up concerns**	Resolve outstanding risks with the counterparty
9	**Monitoring updates**	Track news, events and personnel changes
10	**Re-diligence**	Periodic deep re-evaluation, typically annual or semi-annual

Source: Digital Asset Research. Reports usually contain confidential counterparty data and require consent to share.

"The checklist is the start of the diligence process, not the completion. 'Do you have a SOC?' is table stakes for any counterparty, but you then have to take a critical read of that documentation."

Adam Capon, COO, Digital Asset Research

A checklist confirms that a document exists. A deep dive tests what it says and whether it works in practice (Exhibit 9).

Exhibit 9: After 'Do you have a SOC?': checklist versus deep dive

Checklist	Deep dive
SOC report	**Critical read of the SOC:** scope, exceptions, operational implementation, and how it changed from one period to the next
Policies communicated	**Proof of policy:** are the supporting policies comprehensive, and is there evidence they work in practice?
Completed questionnaire	**Tone of engagement:** how does the team respond, and how willing is it to discuss detail?
Team	**Working knowledge:** turnover at management and executive level; can people talk through critical processes?
Everything else	Insurance, financials, beneficial owners, regulatory licences, OFAC checks and more

Source: Digital Asset Research. Examples are illustrative, not exhaustive.

Some answers cannot be documented, only tested. On whether assets are being rehypothecated off-chain, DAR's method is to ask the question very bluntly, and often to ask two or three people in the organisation separately, such as the CFO and the head of custody, and see if their answers align.

"If you don't get consistent, clear, crisp answers, you should start to develop some doubts."

Doug Schwenk, CEO, Digital Asset Research

V. Case Study: FTX Never Passed DAR's Diligence

Why one of the most liquid exchange was never vetted

FTX shows what deep diligence can catch, and why it depends on access. DAR evaluated FTX through its formative years, taking it through a quarterly waterfall that starts with a quantitative look at trade and order book data and moves into a qualitative review of documents and conversations. FTX never made it through.

Most of the industry took FTX's reported volumes, liquidity and order book at face value. DAR did not. Engaged by institutional clients, it worked with FTX's compliance team, which provided preliminary, mostly public-facing materials. DAR came back with concerns (Exhibit 10) and repeatedly used its network to try to get answers. FTX ultimately said it would not provide more.

> **"We never got the qualitative diligence we required to get to a place of comfort, and that's a big warning sign for anyone treating this as a serious counterparty matter."**
>
> **Doug Schwenk**, CEO, Digital Asset Research

Exhibit 10: Concerns DAR raised about FTX

- The role of Alameda Research
- No conflicts policy available for scrutiny
- Lack of critical transparency on insurance, controls and custody
- Limited compliance personnel and processes
- Limited regulatory licences for the markets it aimed to serve
- Reports from former staff of poor risk management, as reported to DAR at the time

Then FTX said "we won't provide" and stopped responding.

Source: Digital Asset Research.

Tone and posture matter

A gap in disclosure is not proof of fraud. Many exchanges are on a growth journey, and a lack of answers can reflect immaturity or negligence. The judgement that matters, in DAR's view, is where a venue sits on a continuum relative to the institutional benchmarks DAR uses, such as Bitstamp, Coinbase, Gemini, Kraken and LMAX, which provide much of this information.

DAR says it identified FTX as an uncreditworthy counterparty roughly 18 months to two years before the exchange collapsed, and none of its diligence clients lost money.

No process catches everything

DAR checks its own record after every major event, and is open about the limits of the method.

> "We have not identified every poor credit risk, but statistically we have identified the biggest risks that led to loss of client money. Every time there's a major event, we look back: did we get it right? You won't catch them all."

Doug Schwenk, CEO, Digital Asset Research

> "When it is too good to be true, it may be too good to be true. Put the greatest scrutiny on the counterparties that give you the best liquidity and the best terms, and make sure they have the institutional pillars to back that up."

Doug Schwenk, CEO, Digital Asset Research

VI. A Framework You Can Use

Screen, deep dive, monitor, escalate

The two approaches fit together in four steps (Exhibit 11). A broad score screens the whole market down to a shortlist. Deep diligence tests the few venues you will actually use. Monitoring keeps both current, because a vetted exchange can deteriorate within days: track score changes, news and personnel moves, ask why when something changes, and re-run deep diligence periodically. When time, access or expertise runs short, escalate to specialists.

Exhibit 11: Screen, deep dive, monitor, escalate

Step	What it means	Led by
01 Screen	Shortlist from the full universe using Trust Score and its component breakdown.	CoinGecko
02 Deep dive	Test operations, financials, compliance and regulation on the shortlist.	DAR
03 Monitor	Track score changes, news and personnel moves; ask why when something changes.	Both
04 Escalate	Call in specialists when time, access or expertise runs short.	DAR

Source: CoinGecko and Digital Asset Research.

The bar is also likely to rise. Doug Schwenk expects regulatory scrutiny of the industry to increase in the US after the midterm elections, raising the threshold exchanges must meet.

Appendix: Replicating the Screen

Run your own screen with the CoinGecko API

Every CoinGecko figure in this report can be pulled programmatically. The endpoints below let you build your own shortlist and a simple weekly monitor (Exhibit 12); the example is illustrative and should be adapted to your own thresholds (Exhibit 13).

Exhibit 12: Useful exchange endpoints

Endpoint	What it gives you
`/exchanges`	trust_score, trust_score_rank, trade_volume_24h_btc for every active exchange
`/exchanges/{id}`	Exchange profile, Trust Score and top tickers
`/exchanges/{id}/tickers`	Pair-level trust_score and bid_ask_spread_percentage; with depth=true, cost_to_move_up_usd and cost_to_move_down_usd (2% depth)
`/exchanges/{id}/volume_chart`	Historical volume, to spot sudden shifts in activity

Source: CoinGecko API documentation. /exchanges data is cached every 60 seconds.

Exhibit 13: Example: screen and monitor exchanges (Python)

```
import requests
    BASE = "https://pro-api.coingecko.com/api/v3"
    H = {"x-cg-pro-api-key": "YOUR_API_KEY"}

    # 1. Screen: every active exchange with its Trust Score
    ex = requests.get(f"{BASE}/exchanges", headers=H,
                      params={"per_page": 250}).json()
    shortlist = [e for e in ex if (e["trust_score"] or 0) >= 9]

    # 2. Monitor: print current scores; re-run weekly and compare with the last run
    for e in shortlist:
        print(e["id"], e["trust_score"], e["trust_score_rank"],
              round(e["trade_volume_24h_btc"]))

    # 3. Drill in: pair-level spread and 2% depth (see Exhibit 13)
    # GET /exchanges/{id}/tickers?depth=true
```

Illustrative only. Demo plans use https://api.coingecko.com/api/v3 with the x-cg-demo-api-key header. See docs.coingecko.com.

Conclusion

The failures of the last four years have taken different forms: an exchange that misused client assets, and a series of hacks that reached record size with Binance in October 2026. What they share is that the warning signs sat beyond headline volume and liquidity.

No single score is enough. A broad, programmatic view such as CoinGecko's Trust Score lets institutions screen the whole market and see quickly when an exchange's profile changes. Deep, relationship-based diligence of the kind DAR runs tests what a score cannot see: custody, balance sheets, governance and how an exchange behaves when asked hard questions.

Used together, and revisited continuously, they turn exchange selection from a judgement on reputation into a documented counterparty decision.

Need exchange data for your own assessment?

Trust Scores, rankings, pair-level spreads and 2% depth, and historical volume for the exchanges CoinGecko tracks are all available through the CoinGecko API. Start free, or talk to our team about Enterprise licensing and SLAs.

coingecko.com/api

Need a deeper diligence review?

Digital Asset Research provides institutional-grade diligence, vetted exchange lists and ongoing monitoring of exchanges and custodians for TradFi and digital asset firms.

digitalassetresearch.com

This report is provided for information only and does not constitute investment, legal or financial advice. The CoinGecko Trust Score is not a credit rating, and naming an exchange is not an endorsement. Views attributed to Digital Asset Research, and statements about DAR's engagements, are DAR's own. [AUTHOR: state any commercial relationship between CoinGecko and DAR.] Third-party figures are cited from the sources shown and may differ by valuation method. CoinGecko data is as of the dates stated and subject to change.