

Is echobit.com safe? TrustSniffer's moderate-trust assessment: 60/100

echobit.com

Verdict

60

OUT OF 100

MODERATE TRUST

echobit.com is moderately trusted.

Most signals looked ordinary, and some evidence was missing. Read the checks below before you pay or hand over personal details.

Governance Risk

Dynamic Interaction Caution

Assessed 2026-09-30 by automated analysis. Classification confidence 75%.

What this site appears to be

Landing page for 'Echobit' cryptocurrency exchange promoting spot, futures, copy trading and high-leverage products. Claims MSB and VASP registrations and compliance memberships; encourages downloading app and registering. Structural risk: custodial deposits and leveraged trading with unverifiable on-page evidence of regulatory credentials or independent audits.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

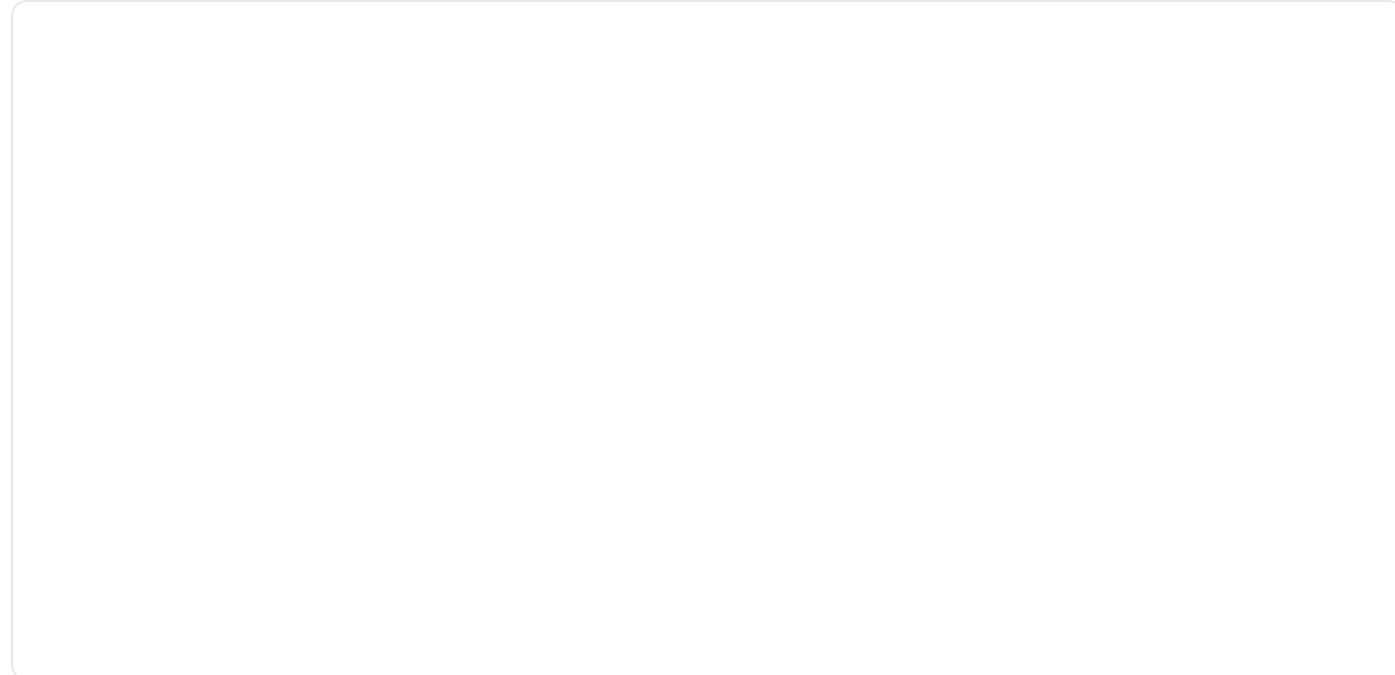
At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 0 reports; shared hosting inflates reports	CLEAR
Domain age	22 years old Registered history	CLEAR
Web archive	Archived since 2001 537 snapshots	CLEAR
Certificate	Encrypted connection Issued by Amazon RSA 2048 M04	NOTED

The page as captured

<https://www.echobit.com/en-us>



What echobit.com served when TrustSniffer captured it on 2026-09-30. The page may look different now.

Key findings

- Automated classification: Governance Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2001.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

Echobit is a cryptocurrency-exchange landing page presenting spot and futures markets, copy trading, an earn area, app-based registration, and leveraged digital-asset trading; its apparent business model involves users depositing assets into a platform-controlled trading environment.

Scam/Impersonation Risk

No blacklist, phishing, malware, brand-impersonation, or conflicting-identity indicators were observed, so no direct scam or impersonation contradiction is established. The principal concern is the operating model: the site requires custodial deposits before service, while the available page evidence does not independently substantiate how customer funds are controlled, how value flows through the platform, or whether the stated compliance framework has been audited. This supports a verification-before-commitment posture rather than a finding that the site is fraudulent. The domain also shows sustained historical continuity, which is a positive provenance signal but does not independently verify the current operator.

EVIDENCE

- The homepage presents a custodial exchange model in which registration and trading follow the sequence “Download–Register–Trade,” with customer assets used within the platform-controlled service.
- Domain registration records show registration on 27 September 2004, an age of 22.02 years, and Name.com, Inc. as registrar.
- Historical records show 537 snapshots spanning 2001–2026, covering 26 years of observed continuity.
- External reputation checks recorded zero malicious and zero suspicious detections, with no external blacklist or Google Safe Browsing malicious finding; the site was also within the global top one million traffic domains.

Regulatory Verification Notes

The homepage claims Money Services Business licensing in the United States and Canada, including FinCEN and FINTRAC references, and claims Virtual Asset Service Provider registration in the Czech Republic. Those are material regulatory representations, but the supplied page evidence does not include registration numbers, independently verifiable certificates, or audit documentation; the legal identity connecting those claims to a real-world operator therefore remains unverified. This is a regulatory-transparency gap, not an identity contradiction. Domain continuity, established traffic presence, valid transport encryption, and stable mainstream hosting provide supporting legitimacy context, while the use of domain privacy remains an administrative limitation rather than proof of wrongdoing.

EVIDENCE

- The homepage’s “Compliance & Security” section makes the United States, Canada, and Czech Republic MSB/VASP claims but does not display registration identifiers in the captured content.
- The site is served on AS16509, AMAZON-02 – Amazon.com, Inc., US.
- The transport certificate is issued by Amazon RSA 2048 M04, uses DV validation, and is valid through 13 April 2027.
- The domain is registered through Name.com, Inc., with the registrant information protected by Domain Protection Services, Inc.

What to Verify Next

Before any substantial financial interaction, the claimed MSB and VASP registrations should be matched to the exact legal entity, registration number, jurisdiction, and permitted activities in the relevant official registries. The operator’s legal name, custody arrangements, withdrawal controls, fee schedule, dispute process, and customer-asset protections should be obtained from the site’s formal legal documentation and independently confirmed through an offline or otherwise trusted channel. Initial exposure should remain limited until those checks are complete.

EVIDENCE

- The homepage makes specific regulatory claims but the captured content does not provide registration numbers or documentary proof.
- The service directs visitors toward app download, registration, and trading, making confirmation of the contracting entity and withdrawal terms directly relevant before funding.
- Dynamic testing recorded three non-whitelisted external XHR requests, three non-whitelisted external POST requests, and eight console errors across two successful runs; these observations warrant confirmation of the endpoints involved before sensitive transactions.

Summary Verdict

Echobit presents a **moderate-trust posture** with meaningful evidence of domain continuity, operational presence, and clean direct-reputation results, but with legitimacy constrained by an unverified operator identity and an inherently high-consequence custodial business model. No direct scam or impersonation contradiction was observed; the appropriate conclusion is an established-looking but not independently authenticated exchange requiring proportionate diligence for sensitive or high-value use.

Infrastructure Integrity

The site is protected by AWS CloudFront CDN/WAF infrastructure, and all observed addresses were CDN edge servers rather than identified origin candidates. This reduces direct exposure of the hosting origin and is a mitigating infrastructure control, but it does not establish the legitimacy of the operator or the safety of deposited assets.

Closing Assessment

Prospective users should complete the independent entity, licensing, custody, and withdrawal checks before making high-value deposits or undertaking sensitive financial activity.

Written analysis generated 2026-09-30 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by page content, several checks together.

01 Page content

- The review of the page content rated it high risk.
Page content rule:PAGE_RISK_HIGH
- The page shows few of the signs expected from a trustworthy operator.
Page content rule:PAGE_TRUST_QUALITY_LOW
- The page content shows three or more warning signs that deceptive sites commonly use.
Page content rule:PAGE_RED_FLAGS_STRONG

02 Several checks together

- No external feed lists the site, but its own page content reads as risky.
Several checks together rule:HYB_POSITIVE_EXTERNAL_NEGATIVE_PAGE

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of echobit.com.

- The request stayed on echobit.com. It was not redirected to another domain. CLEAR
- Registration is published under Name.com, Inc.. CLEAR
- DNS for this domain is served by awsdns-12.org, across 4 name servers. NOTED
- The registration is paid up to 2027-09-27. NOTED
- The earliest public archive of this site is from 2001-06-11. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Name.com, Inc.
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	3.174.113.19
Name servers	NS-1123.AWSDNS-12.ORG, NS-1958.AWSDNS-52.CO.UK, NS-56.AWSDNS-07.COM, NS-824.AWSDNS-39.NET
CDN / edge network	Detected (aws_cloudfront)
Resolved IP addresses	5
Edge IP addresses	5
Likely origin IP addresses	0
SSL issuer	Amazon RSA 2048 M04
SSL expiry	2027-04-13
Domain age	22.02 years (continuous registration)
Domain expiry	2027-09-27
Archive first seen	2001-06-11
Archive snapshots	537

About this assessment

A trust score summarises the evidence TrustSniffer could collect about echobit.com at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/echobit.com> · assessed 2026-09-30