

Is cqyanran.com a scam? TrustSniffer's high-risk assessment: 0/100

cqyanran.com

Verdict

0

OUT OF 100

CRITICAL RISK

cqyanran.com shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 50%.

What this site appears to be

Chinese-language marketing/landing page for a "TPWallet" branded crypto wallet app offering multi-chain support, DApp browser, NFT features and buy-with-card on-ramp. Contains many blog posts and guides about earning, airdrops and mining; lacks visible verifiable audits, legal/regulatory claims, or clear ownership disclosures.

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 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	4.3 years old Registered history	CLEAR
Web archive	Archived since 2023 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://cqyanran.com/>

404 Not Found

nginx

What cqyanran.com served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2023.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

The website is a Chinese-language promotional landing page for “TPWallet,” presenting a downloadable cryptocurrency wallet with multi-chain asset support, a decentralised-application browser, NFT functionality, card-based crypto purchases, and related earning, airdrop, staking, and mining content. Its apparent business model is to drive app installation and subsequent cryptocurrency activity or deposits through integrated wallet and financial-services features.

Scam/Impersonation Risk

No confirmed phishing, impersonation, or other identity contradiction was observed, and available external checks did not identify a confirmed malicious or blacklist signal. However, the homepage combines high-stakes financial functionality with weakly substantiated claims: it describes the wallet as “globally leading,” claims service across more than 200 countries and regions, and displays counters for approximately 80K+ daily transactions, 80+ countries or regions, 80K+ global users, and 80K+ supported tokens without supporting evidence. The earning, airdrop, staking, and mining material, together with the apparent requirement for users to install the application and fund crypto activity before receiving service, creates an opaque value flow and a

significant sensitive-interaction concern. These indicators support a critical cautionary posture without, by themselves, proving impersonation or fraud.

EVIDENCE

- Homepage: promotes a wallet, DApp browser, NFT handling, credit-card crypto purchases, and access to numerous blockchain networks and tokens.
- Homepage: displays unsupported scale and usage claims, including 80K+ counters and service coverage across more than 200 countries and regions.
- Earning and mining content: promotes acquisition and earning-related activity without visible independent audit or substantiation.
- Domain registration: registered 2022-05-10 and recorded as approximately 4.28 years old.

Regulatory Verification Notes

The available site content does not identify a verifiable legal entity, licensing authority, registration number, or independent audit supporting the financial and security claims. This is a material transparency and regulatory-verification gap for a service involving crypto purchases, custody-related wallet functions, token activity, and potential deposits; it is not, in isolation, evidence of a scam. The operator's real-world identity remains unverified. A third-party broker-reputation check returned no match, which provides limited contextual reassurance but is not a licensing or regulatory determination. The site's transport security is present, but a domain-validated certificate confirms encrypted transport rather than the identity or authorization of the operator.

EVIDENCE

- About and feature content: provides product descriptions and team-role names but no clearly verifiable corporate entity, regulatory authority, license number, or audit reference.
- Site transport encryption: TLS certificate issued by YR2, validation level DV, valid to 2026-09-26T06:54:46+00:00.
- Hosting resolution: served from AS54801 (ZILLION-NETWORK - Zillion Network Inc., US).
- External broker-reputation context: no matching broker record was returned.

What to Verify Next

Before any sensitive interaction, an independent check should confirm the application publisher, package or signing identity, and distribution record through the official Apple or Google app-store listing rather than through links supplied by the site. The purported operator should be matched to a government or financial-regulatory register, and the service should provide independently verifiable terms governing custody, withdrawals, fees, disputes, data handling, and any earning or mining arrangement. Security claims should be supported by a named audit firm and a report that can be independently located; contact channels should also be confirmed through an offline or independently sourced route.

EVIDENCE

- Homepage: directs visitors toward application downloads and card-funded crypto activity, making publisher verification a prerequisite to installation.
- About and feature content: presents security and scale assertions without a corresponding legal, licensing, or audit record.
- Earning, airdrop, and mining material: warrants independent confirmation of contractual terms, funding mechanics, and withdrawal conditions.

Summary Verdict

The overall posture is critical, with the website unsuitable for sensitive interaction at present. Its identity is not independently verified, and the combination of unsupported financial claims, unclear value flows, and absent substantiation materially outweighs the limited reassurance provided by stable technical operation and the lack of confirmed threat indicators.

Infrastructure Integrity

The site resolves to a single likely origin address rather than a detected CDN edge layer and is hosted through ZILLION-NETWORK, Zillion Network Inc., on AS54801, with registry attribution to AFRINIC and a Seychelles country code. This infrastructure provides limited protective mitigation: it establishes a functioning hosting path but does not demonstrate operator legitimacy, regulatory status, or transactional safety.

Closing Assessment

Activity should remain limited to passive review until the operator, application provenance, regulatory standing, security evidence, and transaction protections have been independently established; credentials, account access, software installation, and financial transfers should not proceed beforehand.

Written analysis generated 2026-08-21 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by registration and ownership.

01 Governance Risk

- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.

Registration and ownership rule:KF_WHOIS_PRIVATE

- The registration record withholds contact details for the operator.

Registration and ownership rule:KF_WHOIS_HIDDEN

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 cqyanran.com.

- The request stayed on cqyanran.com. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by domaincontrol.com, across 2 name servers. NOTED
- The registration is paid up to 2027-05-10. NOTED
- The earliest public archive of this site is from 2023-02-07. CLEAR
- It is hosted on ZILLION-NETWORK, from a server in SC. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	ZILLION-NETWORK - Zillion Network Inc., US
Country	SC
Server IP	156.239.182.2
Name servers	NS63.DOMAINCONTROL.COM, NS64.DOMAINCONTROL.COM
SSL issuer	YR2
SSL expiry	2026-09-26
Domain age	4.28 years (continuous registration)
Domain expiry	2027-05-10
Archive first seen	2023-02-07
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about cqyanran.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.

