Tech Verification Verification Methodology

Last updated: June 12, 2026

This Verification methodology is incorporated by reference into the Unitstake Terms and Conditions [link] and applies to projects seeking to receive a "Verified by Unitstake" badge (the "Verification Badge"). Unitstake may amend, modify, or update this Methodology at any time. Updated versions will be published on the Platform together with the relevant "Last Updated" date.

1. What Is the Verification Badge

The Verification Badge does not constitute any form of endorsement, recommendation, approval, financial analysis, legal opinion, or due diligence in respect of any project. It reflects only that Unitstake has carried out a limited, structured review of specific information submitted by the project against supporting documents and publicly available sources, in accordance with this Methodology.

Verification is paid but a merit-based service. The fact that a Listed Party has paid the application fee does not in any way influence or predetermine the outcome of the verification. The Verification Badge is granted solely based on whether the Listed Party's submitted materials satisfy the criteria set out in this Methodology. Payment of the application fee does not guarantee that the Verification Badge will be granted.

2. Verification Process

The verification process follows these steps:

- **Application.** The Listed Party completes our application form, providing required information and documents, including details about the asset, team background, tokenomics, links to source code and block explorers. The Listed Party is solely responsible for the accuracy, completeness, and authenticity of all materials submitted. A complete and well-prepared application is important for an efficient review.
- **Completeness check.** On receipt of an application, we confirm that all required documents and information have been provided. Incomplete applications are returned to the Listed Party with a statement of what is outstanding. We may request clarifications or supplementary materials at any stage of the review.
- **Review.** Our verification team conducts a structured review of the submitted materials across five areas: Legal, Financials, Team, Reputation, and Technology, each described in detail in Section 3. We may contact the Listed Party by email or telephone to request additional information or clarification. A timely and complete response is critical for an efficient review.
- **Result.** Following the completion of the review, we notify the Listed Party of the result. Projects that satisfy all applicable criteria will be displayed on the Platform with a Verification Badge. Projects that do not meet such criteria, whether due to gaps in submitted materials or failure to satisfy one or more criteria, will not be granted the Verification Badge. A Listed Party may reapply for verification following remediation of the identified deficiencies.

Review timelines depend on the complexity of the project and the completeness of the application, and may range from 5 (five) to 20 (twenty) business days. Please note that incomplete applications, in particular, those lacking information on governance, tokenomics, or technical documentation, may extend the review period.

3. Verification Category

Every project and its associated asset is reviewed against the same standard

Tech Verification. We verify that the project's smart contract exists, that its key parameters match the project's disclosures, and that the source code is publicly verifiable. For projects involving real-world assets, we also assess whether the contract's functional logic is consistent with the investor rights, revenue distribution mechanism, and asset economics described in the project's legal documentation, Whitepaper, and other materials. We additionally review the contract's administrative controls and governance structure to identify centralisation risks that may be material to investors.

CATEGORY	WHAT WE MAY ASK FOR	WHAT WE CHECK
Tech Verification	• Deployed smart contract address(es) with network and token standard • Link to verified source code on a block explorer or public repository • Third-party security audit report (if any) • Vulnerability testing (if any) • Description of contract upgrade mechanism and governance (if applicable)	**Contract existence and disclosure consistency** • That the deployed contract exists at the stated address and that the token name and symbol match the project's disclosures • That the source code is verified on the relevant block explorer • That the contract shows evidence of genuine on-chain activity and is not dormant or inactive at the time of review • That the concentration of tokens held by team wallets and insider addresses is not materially inconsistent with the disclosed allocation **Functional logic and RWA consistency** • That the functional logic of the smart contract is consistent with the investor rights described in the Whitepaper and other project's documentation • That the revenue accrual and distribution mechanism implemented in the contract is consistent with the project's stated asset economics • That any governance, token buyback, redemption, or other corporate action functions present in the contract are consistent with the terms disclosed by the project **Administrative controls and centralisation risks** • That the contract's ownership structure and administrative permissions are identified and disclosed • Whether control over the contract after deployment is held by a single address or distributed via a multisignature mechanism • Whether any single party can unilaterally modify critical contract parameters • Whether the contract includes a token minting function, and if so, whether it is fixed, capped, or subject to unlimited issuance at administrator discretion • Whether the contract includes freeze, block, forced transfer, or token seizure functions • Whether the contract is upgradeable, and if so, who controls the upgrade mechanism and under what conditions upgrades may be performed • Whether a third-party security audit has been conducted and whether the audit report is publicly available

Limitations of Verification. Unitstake does not audit or certify financial statements, conduct independent smart contract security audits, provide legal opinions on token classification, or assess the investment merit, commercial viability, or suitability of any project for any purpose.

Our review of the underlying asset is based on title documents, registry extracts, and other materials submitted by the Listed Party, supplemented by searches of publicly available official sources where accessible. We do not conduct physical inspection of assets, commission independent valuations, or verify asset condition. Where independent registry verification is not practicable, we rely on a signed director's declaration, confirming the presence or absence of encumbrances.

Our review of professional backgrounds is limited to information and documents submitted by the project in the course of verification. We do not conduct independent background investigations.

Our reputation review consists of open-source research conducted at the time of verification. We do not access non-public databases, law enforcement records, or court files, and we do not verify the accuracy of identified publications or conduct our own investigation into the underlying facts.

Our review of smart contract logic is limited to assessing whether the contract's disclosed functions appear consistent with the project's stated investor rights and economic model. It does not constitute a security audit and does not identify all potential vulnerabilities or attack vectors.

So, our review is based on materials submitted by the Listed Party and publicly available sources at the time of review — we do not access non-public databases, law enforcement records, or court files. The absence of adverse findings does not mean a project has a clean reputation or is free of risk. The Verification Badge is not a substitute for independent professional due diligence.

4. Refusal of Verification

Unitstake will not grant the Verification Badge, and may remove the project from the Platform, if:

- The project operates in, or is materially associated with, prohibited categories, including pyramid, Ponzi, or multi-level marketing schemes whose economic model relies primarily on the recruitment of new participants; services facilitating money laundering, terrorist financing, or dealings with sanctioned persons or entities; businesses primarily engaged in illegal goods or services; or projects with no identifiable underlying product, service, or use case beyond speculative token trading;
- The project presents one or more indicators of fraudulent or harmful conduct, including public claims of guaranteed returns or risk-free investment outcomes; material inconsistencies between the token sale terms and the whitepaper disclosures; or a team that cannot be verified;
- The application contains false, misleading, incomplete, inconsistent, or unverifiable information, including information regarding beneficial owners and key individuals; or
- The project's smart contract source code is not publicly accessible or verifiable on the relevant block explorer, or the contract contains undisclosed privileged functions, including the ability to mint tokens without limit or to freeze or seize user balances.

The lists above are indicative and non-exhaustive. Unitstake reserves the right, at its sole discretion, to refuse verification and is under no obligation to give reasons for any such decision.

5. Post-Verification Obligations

The Verification Badge reflects the state of information at the time of review. Listed Parties must notify Unitstake promptly of any material change to the verified information, including changes to corporate structure, key personnel, tokenomics, or technical components.

Unitstake may withdraw, suspend, or modify the Verification Badge at any time and without prior notice, if: the Listed Party fails to notify a material change; Unitstake determines that the underlying information no longer meets its verification criteria; or Unitstake becomes aware of information inconsistent with the basis on which the Verification badge was granted. Withdrawal does not give rise to any right of refund.