DSA / RESEARCH SERIES 2026

Quantstamp: traceable reports need a current-engagement check

Two PDFs linked from the audit service page offer scope and outcome evidence, but their age limits what they say about the team available today.

DSA research, prepared with AI assistance

Published September 5, 2026 | Version 1.0

Public-source research; independent expert review pending

This document reviews cited public evidence. It is not a code audit, a certification, or an endorsement by an appointed expert panel.

Measurements in this report

Directly linked PDFs inspected	2
Sample PDFs with version and outcome evidence	2
Sample PDFs inside preceding 24 months	0
Additional HTML reports rendered and inspected	4
All linked sample artifacts within 24-month window	0

Read online: https://defisec.info/reports/quantstamp-evidence-review-2026

Evidence coverage against the seven criteria

All scores are withheld. These are source-evidence observations, not independent technical assessments.

Technical finding quality | Not scored

Published finding narratives available. Exploits have not been reproduced by DSA.

Depth and threat model | Not scored

Scope and method material available. Test adequacy and omitted threats need expert review.

Scope and version traceability | Not scored

Version or deployed-address anchors are recorded. Independent repository/build validation is pending.

Demonstrated specialization | Not scored

Sampled projects identify relevant technologies. Assigned-team fit remains unverified.

Fix verification | Not scored

Resolution narratives inspected. Accepted risk is kept separate from a verified code fix.

Internal quality control and response | Not scored

No independent internal QA workpapers inspected.

Transparency and conflicts | Not scored

Public identity sources are available. Reviewer and commercial conflict declarations have not been collected.

Selection and original evidence check

We opened the two audit PDFs directly linked from Quantstamp's current audit service page: MakerDAO Liquidations 2.0 and Teku. This is a reproducible link-based sample, not a search for the most recent two reports in the entire portfolio. Both documents were readable and contained repository or code-target information, revision identifiers, finding detail and resolution statuses.

Age changes the inference

The MakerDAO document includes a March 2021 revision history; the Teku report is dated November 5, 2020. Both are more than five years old at the September 2026 check. Their continued accessibility demonstrates historical documentation, but it does not identify the current team or establish current specialization.

This matters to the proposed committee rule requiring reports from three distinct projects in the preceding 24 months. Neither artifact in this particular sample meets that freshness window. That is a gap in the assembled packet, not evidence that Quantstamp lacks newer work. The next step is to request recent comparable reports or locate them through the wider public portfolio.

Different targets, different assurance questions

The MakerDAO report identifies three in-scope Solidity files and records changes to the assessed revision in its timeline. The Teku report concerns an Ethereum client and names Java and Kotlin. Treating both as interchangeable "smart contract audits" would erase an important distinction in engineering scope.

The MakerDAO report includes file hashes, while the Teku report tells readers to use the repository revisions instead. These are different ways of identifying a target. DSA checked the presence of those identifiers; it did not independently rebuild the targets or map them to a live deployment.

Read outcome narratives before shortlisting

Both documents use multiple finding statuses. Acknowledged and mitigated items remain distinct from a verified code fix. A request for evidence should therefore ask which final revision was checked, what remained unresolved and who accepted the residual risk. The presence of a completed audit report is not a statement that the deployed system is free of exploitable conditions.

For a current proposal, request three recent reports matching the intended protocol, identify the assigned reviewers and define the fix-review and regression-testing allowance. The historical samples are useful interview material, but they do not support a present-day price, availability estimate or provider-wide technical score.

Four HTML reports checked after JavaScript rendering

The same service page links four HTML reports in addition to its two PDFs. A plain HTTP text extraction returned only a shell, so we opened all four in a browser: Alchemy Modular Account, Sperax USDs, Tensorplex Stake and Venus Protocol Vaults. Each rendered a scoped code identifier and per-finding outcomes. Their stated engagement timelines end in 2023 or January 2024. All six service-page-linked artifacts therefore fall outside the proposed September 2024 to September 2026 qualification window. This remains a bounded landing-page sample, not a census of the wider certificate portal.

Limits and next verification step

This is a bounded review of public evidence. We did not rerun exploits, inspect private workpapers, interview the assigned audit team or verify current booking availability. The observations describe the cited artifacts and cannot establish the provider's overall defect-detection rate. A procurement decision still needs a scoped proposal, relevant recent work and independent technical review.

Sources and reproducibility

All source checks were made on September 5, 2026. Content hashes identify the retrieved artifacts. Data definitions and the source manifest are available from the report page and the link below.

1. Current audit service and linked PDFs

Official source: quantstamp.com

SHA-256: 67a9ca2d731616473afc24dc05b480e436f5a5092f6f9e0f4819b67752889074

2. MakerDAO Liquidations 2.0 report

Official source: certificate.quantstamp.com

SHA-256: dc98b30953e93dfc67c9b525e3bf78593929267751a9220ce375bc8c2436b2d5

3. Teku report

Official source: certificate.quantstamp.com

SHA-256: 502cd3591359a17ec7d9825b34babbb193af4dd460341f7d216d86c1ff8f80f4

4. Alchemy Modular Account

Official source: certificate.quantstamp.com

SHA-256: cac0a0b9768ab916936f471a8b966fb443dc052150bf6c461f446078d51ad137

5. Sperax - USDs

Official source: certificate.quantstamp.com

SHA-256: 8ac6d26cc0204c365b45a06a89d370612f54682f4dfa04edb4414d91f2391c1f

6. Tensorplex Stake

Official source: certificate.quantstamp.com

SHA-256: 29d8f0570589f4462a76e1c253e587d5817ac90f1a88a672355a6097506b6d72

7. Venus Protocol (Vaults)

Official source: certificate.quantstamp.com

SHA-256: 7b5334f48e35b7e6998115f305355d99d27d3d03131529da707df8c532e19dd8

Data and methodology

https://defisec.info/downloads/research/evidence-measurements-2026-09-05.json

Selection rules, HTTP results, source hashes, and original counts are recorded in the accompanying data. The research used AI assistance. No independent technical committee review is claimed.

https://defisec.info/methodology