OpenZeppelin: tracing the ZKsync OS review to scope and fixes

A published Rust review provides scoped revisions and issue updates; its exclusions matter when assessing relevance to a new engagement.

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

Initial revisions identified in first two scope blocks	2
Report-stated issues	22
Report-stated resolved issues	16
Report-stated partially resolved issues	1

Read online: https://defisec.info/reports/openzeppelin-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.

Why this artifact was selected

We followed OpenZeppelin's research index to the ZKsync OS audit as a purposive example of protocol-level Rust work. It is not claimed to be the latest audit or a representative sample of all OpenZeppelin engagements. The article is dated October 15, 2025 and states a June 9 to June 20, 2025 audit timeline.

Original traceability check

The first two scope blocks identify repository revisions 96d9d37 and 0563213 and enumerate directories under review. This gives a reader a starting point for reconstructing the assessment. The source explicitly excludes two account-model files because account abstraction was not supported at that point. A reference to the project name alone would conceal that boundary.

Our check records two named initial scope revisions in those blocks, a directory-level scope, technical issue narratives and per-issue updates. We did not independently resolve every short hash, reproduce the build or verify that the final deployed system matches either assessed revision. These are evidence-presence observations.

A summary count is not a closure decision

The report's summary states 22 issues, with 16 resolved and one partially resolved. Those figures come from the provider's report, not from a new vulnerability test by DSA. Readers must inspect individual statuses before treating the engagement as complete.

For example, the gas-accounting discussion carries an acknowledged, unresolved update, while other findings link to corrective pull requests and commits. The distinction is useful: acknowledging a risk, scheduling a change and verifying a fix are separate outcomes. A shortlist comparison should preserve the difference instead of reducing all three to an audit-completed badge.

Fit for a proposed engagement

This artifact supplies evidence of a published review concerning Rust execution infrastructure and EVM behavior. That supports a targeted discussion about protocol internals. It does not automatically demonstrate equal depth for every Solidity application, non-EVM chain or financial mechanism.

Before commissioning work, request two more recent comparable project reports, the people assigned to the engagement, how reviewers will model trust boundaries and the final version-validation procedure. Ask how unresolved deviations from the expected execution specification will be recorded and who can accept them. No technical score is issued from this single sample.

Five recent project candidates

The expanded packet includes Miden, StableGold, TxFlow, Across v5 and the Ross Protocol contracts-v5 review. The official pages are dated August 17 to August 26, 2026. Each has explicit scope and issue-update material. The TxFlow scope uses a deployed contract address; the other four identify repository commits. These different anchors must not be collapsed into a single commit-present flag. Index ordering selected the candidates, not a claim to have enumerated every OpenZeppelin engagement.

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. OpenZeppelin ZKsync OS audit

Official source: www.openzeppelin.com

SHA-256: 02eedac03d6f177cc389c6a828d4a15e347a6ca3b131b34072ed1632de6d2887

2. Official research index

Official source: www.openzeppelin.com

SHA-256: 8987a14adf5e106ceed163b87deaab2b2aa6d1235f1d97fcf2f3936d7fbb7e6b

3. Published audit process

Official source: www.openzeppelin.com

SHA-256: 14277e05b221f30ffa19aa08891b32b921dcaf844ae040b726b50cb83357f5d0

4. miden smart contracts audit

Official source: www.openzeppelin.com

SHA-256: 632decfd12453e01c98a02679fdbd85bcd740bb601820185687870f691c5488f

5. stablegold audit

Official source: www.openzeppelin.com

SHA-256: 829c7cd3ef566f872dcb4071676e2c57d1fe4be8b10bc7d099fea56473c07d6a

6. txflow security audit

Official source: www.openzeppelin.com

SHA-256: 5c28ea5d09b9787d6c862fbc0d639808b0fb5fff02586c381a585c57303049cf

7. across protocol v5 bridging system audit

Official source: www.openzeppelin.com

SHA-256: 0877575dfd549ffe84e4649c6255b7cf161fb3dfd6c907a6ad01d614dbbbf527

8. contracts v5 audit

Official source: www.openzeppelin.com

SHA-256: 61ab0f61244b136825281e6892c22de8fe35286a2c889214fa65e73c5f1ee100

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