FP Complete

Hedera Scheduled Transactions

AUDIT REPORT

Customer Name: Hedera Hashgraph

Version: 1.0

Submitted to: Hedera Hashgraph

Table of Contents

Prologue

This report is designated for **external distribution**, in accordance with the disclaimer below.

Disclaimer

This report is authorized for external distribution. This report is presented without warranty or guarantee of any type.

This report touches aspects of both the code itself and the architecture. Information for the architecture is gleaned from the whitepaper, website, and discussions with Swirlds members.

THIS REPORT IS UNCORRECTED AND INCOMPLETE, IS BASED ON INCOMPLETE INFORMATION, AND IS PRESENTED WITHOUT WARRANTY OR GUARANTY OF ANY TYPE.

This report is a copy of a work in progress. It lists the most salient concerns that have so far become apparent to FP Complete after a partial inspection of the engineering work. The inspection is ongoing, so further concerns are likely to arise. Corrections, such as the cancellation of incorrectly reported issues, may also arise. Therefore, FP Complete advises against making any business decision or other decision based on this report.

FP COMPLETE DOES NOT RECOMMEND FOR OR AGAINST THE USE OF ANY WORK OR SUPPLIER REFERENCED IN THIS REPORT.

This report focuses on the technical implementation as provided by the project's implementors, based on information provided by them, and is not meant to assess the concept, mathematical validity, or business validity of the project. This report does not make any assessment of the implementation or the project regarding financial viability, nor suitability for any purpose.

While this assessment when complete might be described as an "audit," no official standard exists for an audit of this nature. The word "audit" does not imply compliance with an accounting standard or other standard and is used informally here. FP Complete has not been given access to nor reviewed all aspects of the project and the engineering decision process underlying all the work. This report likely contains errors due to incomplete information as well as simple misunderstanding. This report may include references to problems that do not in fact exist. Meanwhile, the work referenced may or may not contain undetected or unreported problems. FP Complete has not had independent and unfettered access to all the relevant materials. Nor has a "whistleblower" or other process been provided such that any known problem could be reported and included herein.

Some technical decisions in the engineering work were made due to historic reasons, time constraints, budget constraints, or other constraints. Therefore, the presence of a concern or "flag" in this report does not imply improper conduct or lack of skill by the implementer or manager or any party.

NO ATTEMPT IS MADE OR IMPLIED TO JUDGE ANY PERSON, TEAM, COMPANY, OR OTHER PARTY.

Source Material

For this report, the FP Complete team has reviewed the Hedera Token Service, which is part of the services code of the Hedera node. The source materials consist of:

- The public documentation available at `https://docs.hedera.com/guides/`

- The `hedera-services` repository at `https://github.com/hashgraph/hedera-services` up to commit SHA `ffb4d7db0f802229a5642642a1353b3f4fa05a07`.

- The `hedera-protobufs-java` repository at `https://github.com/hashgraph/hedera-protobufs-java` for the release `0.13` with commit SHA `164083cdda62bd25ef3acaac72ac26e2a19e0725`.

Furthermore, the audit explicitly excluded:

- Code that is not related to the Hedera Scheduled Transaction service
- Automatically generated code
- DevOps, infrastructure, and network architecture
- Technical leadership
- Applicability for business use-cases
- Hiring

Considerations

After fixes, previously identified issues have been resolved. For brevity, those issues are not included in this report.

Legend

This report classes findings into two categories:

- **Red flag** Confirmed issue which should be addressed immediately
- **Yellow flag** Potential problem without a clear or immediate exploit

This report does not include past findings of the repository `hedera-services` raised in previous audits. Instead, we list unresolved and partially resolved flags that comment about production code of Hedera Scheduled Transactions.

Executive Summary

This report contains 0 red flag issues and 1 yellow flag issue. These issues remain partially resolved or unresolved at the time of writing.

Unresolved and Partially Resolved Findings

This section lists all partially resolved and unresolved findings.

Yellow flag: Static analysis

Reproducible in commit: ffb4d7db0f802229a5642642a1353b3f4fa05a07

Impact

No direct impact.

Situation

The static analysis tool Infer was used on the code base. Specifically, the command `infer --` `./mvnw clean compile` was run to generate a report.

Issue

Infer reports numerous warnings which are attached in the asset `infer.txt`. This file only contains findings about production code, test code issues are excluded. The summarized findings are:

- 20 potential thread violations
- 8 potential null-dereferences
- 4 potential inefficient keyset iterations
- 3 potential resource leaks

Recommendation

The static analysis issues should be fixed where applicable. We recommend running the Infer tool as part of the CI so that these classes of error are caught sooner.

Resolution

A tracking issue has been created in #1230. It has been found that reported resource leaks in `try-with-resource` statements are false positives. Some static analysis issues have been fixed in PR #1242.