Best Effort Review Report

Axelar solana-gateway (2)
Solana program

by ARDA

on October 15, 2025

Table of Contents

Disclaimer 3

Terminology 4

Objective 4

Summary 5

Inherent Risks 6

Disclaimer

The report makes no statements or warranties, either expressed or implied, regarding the security of the code, the information herein or its usage. It also cannot be considered as a sufficient assessment regarding the utility, safety and bugfree status of the code, or any other statements.

This report does not constitute legal or investment advice. It is for informational purposes only and is provided on an "as-is" basis. You acknowledge that any use of this report and the information contained herein is at your own risk. The authors of this report shall not be liable to you or any third parties for any acts or omissions undertaken by you or any third parties based on the information contained herein.

Due to its time-constrained nature, a best effort review might not go in the same security depth as an audit. In particular, it does not include a re-assessment on whether all reported issues are correctly fixed at a frozen, subsequent version of the codebase. Further, issues might not be disclosed even if still open, and inherent risks might not have been investigated.

Terminology

Code: The code with which users interact.

Inherent risk: A risk for users that comes from a behavior inherent to the code's design.

Inherent risks only represent the risks inherent to the code's design, which are a subset of all the possible risks. **No inherent risk doesn't mean no risk.** It only means that no risk inherent to the code's design has been identified. Other kind of risks could still be present. For example, the issues not fixed incur risks for the users, or the upgradability of the code might also incur risks for the users.

Issue: A behavior unexpected by the users or by the project, or a practice that increases the chances of unexpected behaviors to appear.

Critical issue: An issue intolerable for the users or the project, that must be addressed.

Major issue: An issue undesirable for the users or the project, that we strongly recommend to address.

Medium issue: An issue uncomfortable for the users or the project, that we recommend to address.

Minor issue: An issue imperceptible for the users or the project, that we advise to address for the overall project security.

Objective

Our objective is to share everything we have found that would help assessing and improving the safety of the code:

1. The **inherent risks** of the code, labelled R1, R2, etc.
2. The **issues** in the **code**, labelled C1, C2, etc.
3. The **issues** in the **testing** of the code, labelled T1, T2, etc.
4. The **issues** in the **other** parts related to the code, labelled O1, O2, etc.
5. The **recommendations** to address each issue.

Summary

Blockchain: Solana

Initial scope

- **Repository:** https://github.com/eigerco/axelar-amplifier-solana
- **Commit:** `4650459d3eb2544b42ed9b5838872085b16fa83f`
- **Path(s):** `./programs/axelar-solana-gateway-v2/`

3 inherent risks

9 issues reported

Some issues could still be open (fix missing or not reviewed).

Severity	Reported
Critical	2
Major	2
Medium	2
Minor	3

We do not disclose the issues of this report.

Inherent Risks

R1: Users have no guarantee that the messages they send to the Gateway will reach the target smart contract on the destination chain.

This is because there is trust that sufficiently many Axelar validators sign the message and that relayers forward the message:

- Sufficiently many Axelar validators should sign the message, otherwise the message won't reach the Gateway on the destination chain.
- Relayers should pick the message from the source chain and inform Axelar validators about it, and once the message is signed by validators, relayers should forward it to the destination chain. Therefore, in the absence of relayers, the message would not reach the destination smart contract on the destination chain.

R2: Users have no guarantee that the messages which are approved in the Gateway are the messages which were effectively created by accounts from another chain.

This is because a message can be approved in the Gateway if it is signed by sufficiently many Axelar validators, and moreover there should be relayers to forward the message from the source blockchain to Axelar network and then to the Gateway. Therefore:

- An erroneous message which was not created on another chain might be approved if for any reason sufficiently many Axelar validators signed it, e.g. if these validators made mistakes or were manipulated.
- A valid message created on another chain might never reach the Gateway if insufficiently many Axelar validators signed it, or if it was not forwarded by relayers.

R3: The following parameters might be set to harmful values: the number of past validator sets that can approve messages, and the delay before which a new validator set can be registered.

This is because Axelar validators are allowed to set these parameters to any values, without any kind of protections, which could be harmful:

- If the number of past validator sets that can approve messages is too big (e.g. 1B), then even after adding numerous new validator sets, an old set, possibly made of unwanted and malicious validators, would still be allowed to approve messages.
- If the delay before which a new validator set can be registered is too small (e.g. 0 seconds), then new validators might be added too frequently, making it hard to keep track of active validator sets: in this case relayers might fail to make users' message approved in the Gateway. By contrast, if the delay is too big (e.g. 100 years), then the most recent validator set would be unable to elect a new validator set in case it plans to go inactive and needs to be replaced.

In practice however, the risk is low, because the choices of parameters result from a consensus between multiple validators of the Axelar blockchain.

Finally, the reason why Axelar does not implement protections directly in the Gateway is to follow the same convention as all the Gateway smart contracts deployed on other chains.