This proposal was co-authored by the L2BEAT governance and research teams.

Abstract

This AIP seeks to propose changes to the structure of the security council so Arbitrum can maintain the “Stage 1” designation as per L2BEAT and not fall back to “Stage 0” designation.

Motivation

On December 7, L2BEAT published an update to the security council requirements for theStages Framework. The requirements were updated after a lot of research and feedback to make Stages more formal and precise.

Rationale

Upgrading the security council as per the Stage 1 requirements set by L2BEAT, will help ensure Arbitrum remains decentralized, but properly secured. See ‘Specifications’ for more details.

Key Terms

Stages:

A framework, inspired by Vitalik’s proposed milestones, that categorises rollups into three distinct stages based on their reliance on these training wheels. You can learn more about the Stages framework here.

Security Council:

A group of 12 individuals who are responsible for addressing risks to the Arbitrum ecosystem through the selective application of e

mergency actions and non-emergency actions. Learn more inthe ArbitrumDAO Docs.

Timelock:

Smart contracts which implement a delay between an upgrade confirmation and execution.

Exit Window:

The actual time users have to exit the system in case of an unwanted upgrade.

Specifications

Arbitrum currently has two multisigs and they both contain the same set of members:

a) A 9/12 multisig with instant upgrade power

b) A 7/12 multisig that can upgrade with a 3+7+3 days delay

While the higher threshold multisig can be classified as a Security Council, the lower one is below the minimum threshold and it’s considered a simple multisig according to the Stages framework introduced above.

For normal multisigs, L2BEAT requires at least a 7 days exit window for users. The current exit window for Arbitrum is 2 days (see this thread for a quick explanation).

Moreover, the higher threshold multisig is supposed to stop malicious upgrades attempted by the lower threshold multisig. However, since the member set is the same, if the lower threshold agrees on something there are not enough members in the higher threshold to stop them, which means that the actual security of the upgradeability mechanism boils down to the 7/12 threshold.

For the above reason, technically, with the updated requirements for Stages, Arbitrum falls back to the Stage 0 designation. Since we know that it takes time to upgrade Arbitrum, we decided to leave the Stage 1 designation with the promise of addressing the above issues in a timely manner. This proposal is about addressing the issues and moving them to be voted on by the DAO.

Proposed Solutions

1. The first solution

would be to remove the lower threshold (7/12) multisig entirely. This can be done in two ways:

- The contract is removed which requires an on-chain upgrade, or,

- The lower threshold multisig increases its threshold from 7/12 to 9/12 which requires no upgrade.

Increasing the threshold gives us the flexibility to restore a lower threshold in the future should the need arise, and it's also a very quick and easy fix since it doesn't require an on-chain upgrade.

On the other hand, removing the dependency on the lower threshold mutlisig for all the contracts in Arbitrum is a broad and potentially risky change. Therefore we suggest raising the threshold for the time being and revisiting the removal of all the dependencies at a later date if needed.

1. The second solution

would be to leave the lower threshold multisig as it is, but to increase the exit window to 7 days. In practice, this involves increasing the L2 timelock delay from 3 days to 8 days, since there is a 1 day max delay to force transactions on Arbitrum via L1 using the 'DelayedInbox'. Increasing the L1 Timelock would not be very beneficial due to delay attacks on the fraud proof systems, since, even with BoLD, the challenge period would end up being up to 16 days.

1. The third solution

, which is not strictly required by the Stages Framework for the Stage 1 designation, is to both remove the lower threshold multisig entirely and increase the L2 Timelock delay so users have more time to exit in case of unwanted upgrades, increasing the security of the system even more.

Steps to Implement

Following a week of discussion of this RFC, the proposal will go for a vote on Snapshot with the following 4 options (as they are or slightly adjusted), and/or any additional ones, should they arise from the discussion during the RFC phase:

1. Increase the threshold from 7/12 to 9/12.
2. Increase the L2 timelock delay from 3 days to 8 days.
3. Increase the threshold and the L2 timelock delay.
4. Make no changes.

Following the temp-check, if any of the aforementioned options apart from No.4 is the most popular, the proposal will move to on-chain vote to execute the proposal.

Overall Cost

There's no overhead to the DAO for the implementation of this proposal.

Timeline

RFC -

January 11th to January 18th

Snapshot -

January 18th to January 25th

On-Chain Vote:

January 30th to February 13th

Execution Delay:

- February 13th to February 16th - L2 Waiting Period
- February 16th to February 23rd - L2-to-L1 Message
- February 23rd to February 27th - L1 Waiting Period

Please note the aforementioned timeline is tentative and the actual timeline might be slightly different.