Security Research Labs

PR #2341 review

A summary of a security review of removing the dex saving functionalities from the Acala chain, implemented in PR #2341.

V1.1, September 19, 2022

Mostafa Sattari mostafa@srlabs.de

Bruno Produit bruno@srlabs.de

Regina Bíró regina@srlabs.de

Content

1 Context

On August 4, 2022, Acala introduced a new iBTC/aUSD liquidity pool via a proposal [1]. On August 14, the pool went live resulting in erroneous minting of considerable amount of aUSD tokens as a reward to the liquidity pool's contributors. Some opportunistic users/bots took advantage of this issue and claimed their (erroneously high) rewards.

2 Incident overview

Acala Network uses the incentive program [2] to attract more liquidity and lock them in the pools. This is mainly implemented by the incentives pallet (modules/incentives) [3].

The core logic of the pallet is accumulating rewards periodically on every block initialization. It is done so by specifically calling two functions:

- *accumulate_incentives*: accumulates incentive rewards of multi-currencies
- *accumulate_dex_saving*: accumulates dex saving rewards (stable currency) for dex pool

The above-listed functions calculate the rewards for each pool based on the configured parameters. The *accumulate_incentives* function uses *IncentiveRewardAmounts* specifically, which is a mapping from the *Pool* and *RewardCurrencyId* to the *RewardAmountPerPeriod*. The function *accumulate_dex_saving* however uses *DexSavingRewardRates* to calculate the dex saving rewards. These two reward parameters take a role in specifying the amount/rate of reward issuance for these two types of incentives.

The erroneous minting of aUSD on Acala was therefore caused by the misconfiguration of the *DexSavingRewardRates* parameter for the incentives pallet which should have prevented the misconfiguration from taking effect. The misconfiguration was introduced in council motion #107 [4], which was put to vote at block #1613969 and approved at block #1618651.

3 Proposed fix

After being notified by a network contributor, the Acala team started the investigations on the incident and paused the swap operations through a governance proposal. During their root cause analysis [5], Acala identified the above-mentioned misconfiguration issue which was corrected via another governance proposal.

Acala's proposed fixed is contained in PR #2341 [6]. In this pull request, the *accumulate_dex_saving* function is completely removed, as well as the *update_dex_saving_rewards* function. Furthermore, on the next runtime upgrade the dex saving reward configuration (*DexSavingRewardRates*) is completely removed.

These actions will result in complete removal of the dex saving rewards in the incentives pallet and hence preventing any aUSD being minted as dex saving rewards.

4 Current state

The current state has the *DexSavingRewardRates* set to 0, meaning that the accumulation has stopped. If dex operations are resumed, the chain would not continue to mint aUSD, but proposals changing the current state could still be accepted in the future. The aUSD transfer paused at block #1639493, stopping all the minting.

5 Conclusion and further recommendations

As the proposals do not go through audits as opposed to the code implementing the core logic of Acala, we suggest creating a testing environment for important proposals, such that the technical and economic impact of each proposal can be measured. Another possibility would be to conduct an experiment to see whether a simulation tool for proposals is feasible to implement. This would allow for a supplementary economic check on proposals.

This PR fixes the issue correctly, and we did not identify other similar issues. The Acala team is planning to implement further sanity checks in the Honzon core logic to prevent similar minting issues in the future.

6 Bibliography

[1] [Online]. Available: https://acala.discourse.group/t/list-ibtc-ausd-pair-on-acala-swap-and-incentive-program-for-liquidity-providers/1122.

[2] [Online]. Available: https://docs.acalaswap.app/overview/incentive-program.

[3] [Online]. Available: https://github.com/AcalaNetwork/Acala/blob/72c01a9fb3a404f92687f8c739c9594255ef8b14/modules/incentive

[4] [Online]. Available: https://acala.subscan.io/council/107.

[5] [Online]. Available: https://acala.discourse.group/t/08-14-2022-incident-on-chain-trace-results/1134.

[6] [Online]. Available: https://github.com/AcalaNetwork/Acala/pull/2341.