Change Review – SPL Stake Pool 2023/11

Neodyme AG

2023-11-14

Contents

Introduction

As part of the Solana peer review process, Neodyme was engaged to do a review of a pull requests to the SPL stake pool program. In particular, the following pull requests have been reviewed:

Title	Link
stake-pool: Allow removal of force-destaked validator	https://github.com/solana-labs/solana-program-library/pull/5439
stake-pool: Allow mints with confidential transfer fee	https://github.com/solana-labs/solana-program-library/pull/5610

This is the full set of changes since the last audit by Neodyme, as of November 14th, 2023 (commit hash `6ed7254d1a578ffbc2b091d28cb92b25e7cc511d`). No issues have been found with the listed changes. The program is still in active development, any changes past this point are out of scope for this report.

Project summary

The SPL stake pool program provides the ability for pooling together SOL to be staked by an off-chain agent running a Delegation Bot. This bot redistributes the stakes across the network and in order to maximize censorship resistance and rewards.

SOL token holders can earn rewards and help secure the network by staking tokens to one or more validators. Rewards for staked tokens are based on the current inflation rate, total number of SOL staked on the network, and the individual validator's uptime and commission (fee).

Stake pools are an alternative method of earning staking rewards. This on-chain program aggregates SOL to be staked by a staker, allowing SOL holders to stake and earn rewards without directly managing their stakes.

Contract expectations

Users of the stake pool should be able to rely on the following two properties:

1. Safety: It is always possible to withdraw the stake deposited. Users must receive stake proportional to their pool share.
2. Fairness: Every user should receive the same relative rewards, proportional to their stake in the pool.

It is important to note that rewards aren't guaranteed, as the manager of the stake pool can always unstake the managed stake accounts. However, under the assumption of a well-behaved manager the "fairness" property ensures that all rewards will be distributed fairly among the users of the pool. The "safety" property ensures that if a user becomes dissatisfied with the manager's decisions, they can decide to leave the pool and retrieve their share of stake at any time.

Additionally, the manager should always receive the fees configured for possible user actions. There should be no way for any user to bypass the configured fees.

Methodology

Neodyme's audit team performed a comprehensive examination of the changes included in the aforementioned pull requests for the SPL stake pool program. The audit team, which consists of security engineers with extensive experience in Solana smart contract security, reviewed and tested the code, paying special attention to the following:

- Ruling out common classes of Solana contract vulnerabilities, such as:
  - Missing ownership checks
  - Missing signer checks
  - Signed invocation of unverified programs
  - Solana account confusions
  - Redeployment with cross-instance confusion
  - Missing freeze authority checks
  - Insufficient SPL account verification
  - Missing rent exemption assertion
  - Casting truncation
  - Arithmetic over- or underflows
  - Numerical precision errors
- Checking for unsafe design which might lead to common vulnerabilities being introduced in the future
- Checking for any other, as-of-yet unknown classes of vulnerabilities arising from the structure of the Solana blockchain
- Ensuring that the contract logic correctly implements the project specifications
- Examining the code in detail for contract-specific low-level vulnerabilities
- Ruling out denial of service attacks
- Ruling out economic attacks
- Checking for instructions that allow front-running or sandwiching attacks
- Checking for rug pull mechanisms or hidden backdoors

Scope

The audit encompassed the pull requests (patches) listed in “Introduction” (PR numbers 5439, 5610) and fixes for reported issues.

Peer review result: Overview

The audit team reported a total of 0 findings, of which (with decreasing impact)

- 0 were critical,
- 0 were high,
- 0 were medium,
- 0 were low, and
- 0 were informational.

Peer review result: Detailed description of the changes

Allow removal of force-destaked validators (PR #5439)

This PR affects the logic of the `RemoveValidatorFromPool` instruction. This instruction does not modify the accounting state of the stake pool. The main security concerns for this instruction are that

(a) Only the staker authority is allowed to remove validators
(b) Funds in stake accounts associated to the removed validator are returned to the pool before the validator record is removed
(c) The validator can be removed using the `CleanupRemovedValidatorEntries` instruction at some point in the future

Condition (a) is verified by checking for the signature of the staker.

Condition (b) is guaranteed by setting the state of the validator to either `DeactivatingAll` or `DeactivatingValidator`, depending on the transient stake state.

Condition (c) is ensured by deactivating all associated stake accounts, so that they can be later merged into the reserve.

The PR changes `RemoveValidatorFromPool` to allow the removal of transient stake accounts or validator stake accounts which are already deactivating/deactivated. This is implemented by skipping deactivation if a deactivation epoch is already set (as re-deactivation is not allowed by the Solana stake program). As this change only bypasses unsuccessful deactivation attempts, condition (c) remains unaffected. The other security considerations remain intact by this change, as they do not rely on the concrete state of the involved stake accounts. This change therefore introduces no vulnerabilities.

Allow mints with confidential transfer fee extension (PR #5610)

The stake program uses a whitelist of allowed extensions for the token mint of the pool token. This is required, as token extensions can fundamentally alter the behaviour of token transfers, such as blocking them entirely. Since the `Withdraw` instructions transfers pool tokens to the manager, blocked transfers would allow the manager to take user funds hostage.

The PR whitelists the extension `ConfidentialTransferFeeConfig` for the pool token mint. This is safe, as `ConfidentialTransferFeeConfig` on the mint does not alter the behaviour of normal token transfers or burns.

Neodyme AG

Dirnismaning 55
Halle 13
85748 Garching
E-Mail: contact@neodyme.io

https://neodyme.io