keyko

Pirex

Contracts Audit

March 2022

Task

We were tasked with performing a Smart Contracts security audit for the core business logic of “Pirex”

Mission

The intention was to have an initial review of the contracts to identify:

- Architecture problems
- Code issues
- Suggestion of improvements

Code

The commit hash audited was: 032604740a78bce49ad569e2114c998da20cf290

Summary

When Cvx is deposited to PirexCvx, it will be locked using CvxLocker. The depositor gets PxCvx, which can be used to redeem rewards or unlock the Cvx. The depositor can choose to auto-compound the rewards using UnionPirexVault, which relies on “distributor” to collect the rewards.

Static Analysis

We realized a static analysis with mythril and slither.

- Mythril: “control flow depends on block.timestamp”
- Slither complains about re-entrancy and style issues (PirexCvx.setContract)

Manual Review

We realized a manual review of the contracts about the following topics:

- PirexCvx
- PirexCvxConvex
- PirexFees
- PxCvx
- UnionPirexStaking
- UnionPirexStrategy
- UnionPirexVault

Issues Found

Category	Issue	Suggestion
PirexCvxConvex	The locked amount isn't necessarily optimal, instead the outstanding amount is unlocked as early as possible ● For example there is 10 upCvx for epoch 20, and there's 15 Cvx unlocked at epoch 15, then the 10 Cvx will be unlocked for the 5 epochs…	Unlock only the amount that is necessary in each epoch. Not sure if it's easy to do
UnionPirexStaking	notifyRewardAmount: ● If it's called twice in succession, the reward rate doubles	Looks like computing the rate shold be done differently if \`block.timestamp >= periodFinish\` If this actually is an error, you should check the test coverage…
PirexCvx	initiateRedemptions ● If the fee is zero, it will revert ● Probably also won't work if the fee is 100%	Should work even if fee is set to zero

Issues Found

Category	Issue	Suggestion
PirexCvx	claimMiscRewards - If the list of reward tokens has duplicate token (should be impossible), or otherwise the token balances have dependencies - And in addition, PirexCvx contract is set to be recipient of rewards - Then the reward amounts will get messed up	Unlikely to cause any issues, but it would be better if it was impossible…
Style issues	- initialize variables - Fix compiler warnings - UnionPirexVault.sol:55: comment has wrong type	

Contact & Info

How you can reach us...

Email:	info@keyko.io
Web:	www.keyko.io
Address:	Keyko GmbH Rote Trotte 9 CH-6340 Baar Zug Switzerlan

keyko

Keyko 2020 © All Rights Reserved