Current (Gibraltar) Ltd: Smart Contract Audit Final

Sarah Gray
August 13th, 2018
sarahg.gray@gmail.com

Table of Contents

Summary

The contract has followed the recommendations in the previous audit, as well as made additional changes for readability and intent. The tests are clear and cover each use case. I do not see any issues with deploying this contract as stands.

Code Dependency Changes Since Last Audit

Since the previous audit, the author has slightly modified open-zeppelin's Ownable.sol to be called Custodial.sol and take an address in the constructor rather than depending on *msg.sender*. Other than accepting a constructor argument and changing some language, all behavior is the same as the open-zeppelin Ownable.sol contract, so I have not given that contract an additional audit, other than reading it side-to-side with its Open Zeppelin counterpart to confirm it didn't change behavior from the original.

The author also made modifications to open-zeppelin's Pausable.sol and PausableToken.sol contracts so they inherit from the Custodial.sol contract and provide a constructor that takes the custodial address. This behavior also did not get (and in my opinion does not need) an additional audit. As with Custodial.sol, I viewed both Pausable and PausableToken side by side with their open-zeppelin counterparts to confirm the existing behavior remained the same, with the exception of its new parent & constructor.

Passing in an address to Custodial.sol allows for a greater level of explicitness in deployment.

Contracts covered

This follow-up covers the CurrentToken.sol contract on the develop branch at [f29cdaaa5b4f54ce868ab4e5e689a96a92138b15]

Recommendations Summary

- The tests are clearly delineated one use-case per test, and go through each address in the paused and nonPaused states
- The contract decides to allow *transfer* to error out rather than check balance up front: this is reasonable. This could have gone either way, the benefit of this way is there is now clear documentation around intent; and less code.
- max-size is now hard-coded to 255, which is more clear on intent and uses less code.
- The contract is deployed using a custodian address, making ownership and expectations around pausing/unpausing explicit.
- There is inline documentation on the code which makes intent and readability clear.
- The tests now provide a single explicit use-case for each condition under test.