CRNC Token Audit

August 10, 2018

Table of Contents

Contracts covered

This audit covers the following contracts at commit 57ecac9b:

- CurrentToken.sol
- PausableToken.sol
- Pausable.sol
- Custodial.sol

Summary

The CRNC token is a simple extension of the OpenZeppelin ERC-20 StandardToken implementation. The token inherits from PausableToken, a slightly customized version of OpenZepplein's PausableToken. This customization was necessary in order to inherit from Custodial rather than Ownable, which allows the custodial address to be provided in the constructor, rather than automatically setting the contract owner to the address of the deployer. The token contract's custom functionality is related to providing token holders with the ability to transfer tokens to more than one address at a time. Additionally, it allows three specific addresses to transfer tokens when the tokens are otherwise paused.

Showstoppers

There are no known issues that would prevent this contract from being deployed and work as expected.

Concerns

There are no concerns with this implementation provided that the contract owner's private key is kept secure.

Recommendations

There are no recommendations.

Commendations

Using the latest stable version of Solidity, along with diligent use of require to assure proper function input.

Using OpenZeppelin's SafeMath to avoid integer overflow and underflow bugs.