Smart Contract Audit

Sovryn Genesis Sale

Franklin Richards

15th January 2021

Index

Note: Some threat levels or headings might be empty if there is no vulnerability/updates/suggestions found.

Introduction

The contract audited here and the supporting contracts is/are:

Started with:
https://github.com/DistributedCollective/Genesis-Sale/blob/ac7b9ef/contracts/main/CrowdSale.sol
Latest:
https://github.com/DistributedCollective/Genesis-Sale/blob/53e53f8/contracts/main/CrowdSale.sol

and was shared by Sovryn for auditing purposes while working with them.

Based on the audit, we were able to find 0 High threats, 0 Medium threat, and 0 Low threat with some other changes in the optimization, readability, typos, and comments section.

High Threats

1. None

Medium Threats

1. None

Low Threats

1. None

Optimization & Readability

1. In line 97, `_minPurchase > 0` would be better for readability.
2. The operation in this could have been done using `depositAllowed` and `msg.value`, thus using calldata (lesser gas usage) and avoiding a division operation as well.
3. Instead of storing `totalTokenSupply` in the contract, the only actual use seems to be in `withdrawTokens()`, which could be done using `balanceOf()` in tokenInstance on `address(this)`.
4. “Only Admins are allowed” or something in the similar context would be better readable error message in `modifier onlyAdmin()`.

Typo’s & Comments

1. Many functions are without any comments. Please make sure every function follows the NatSpec Format.
2. `openzeppelin-contra cts` to `openzeppelin-contracts` in Line 8
3. The comparison of _minPurchase and crowdSaleSupply in lines 98 - 101 is not right, as one would be in the wei of RBTC, and the other would be in Token of CSOV. The comparison, if required should be between `_minPurchase * _rate` and crowdSaleSupply.
4. `onlyOwner` and `saleDone` are modifiers, and could remove the brackets in `withdrawTokens()`. Similar cases in other functions as well, like: saleClosure()

Suggestions

1. As there are no pause functions to pause the sale, it does not make sense to pass parameters in `saleClosure()` and just make the `saleEnded` parameter `true` by calling the function. Almost the same case for `stopSale()`.
2. A better check in here would be to check if the address is non zero, and then add it to admin if the address is a non zero address.

3. A better check in here would be to check if `isAdmin` mapping is true for that address, if it is, then mark it as `false`.