GENEVA
DEVCHAIN

Hands On Code Review results

CONTACT

CHRISTIAN BROILLET

@cbroillet

GENEVA DEVCHAIN

MEETUP

Geneva-DevChain-UserGroup

@GenevaDUG

geneva-devchain

DevchainUserGroup

Introduction

Thanks to Thrivelabs to give us the opportunity to do a code review.

This is **not an official** code review, but a DevChain community “Hands On” code review.

Thanks for the great work of the DevChain community!

Audited Contracts

The audited contracts are in the https://github.com/thrivelabs/contract repository.

The version used for this report is commit :

- TriveToken.sol 37a830f67bdebd7e3397ac249fee912bf8655d7c
- SafeMath.sol b08b564e660852343f376c173cee2381a8560456
- IERC20.sol ec5863df18a624cd5ad3d99a6e83f203fb69695c

Critical Severity

1. No test suit provided.

2. The code doesn’t compile due to lines 55, 57, 59.

High Severity

1. Comment not aligned with code. On line 121 comment stated « on presale minimum required amount =100 ETH ». On line 122, code stated a minimum required amount of 10 ETH.

2. The function createTokens() is too long. It’s not easy to follow the logic.

3. The event generation line 74 should be placed before the return command.

Medium Severity

1. You should first multiply and then divide to avoid losing precision.

2. You should use keyword constant for function that doesn’t modify contract state (line 256).

Low Severity

1. You should import standard library instead of rewriting them.

2. On line 136, revert should be done before (line 119) to avoid losing gas for caller.

3. You should use constructor parameters for presaleStartTime, round1StartTime, round2EndTime variables. This will make the code more easy to test.

Low Severity

4. Don’t create return variable in function definition (line 223) if you don’t use it (line 232). Same for other functions.

5. Use a more recent Solidity version. A lot of bug fix have been made between 0.4.11 and 0.4.18.

6. As _totalSupply is a public variable, there is no need to define a getter.

Notes & Additional Information

1. As code doesn’t compile, we don’t have tested compiled code. We only do the review on reading code.

2. Good to use SafeMath to avoid overflow.

Questions?