Solidity Smart-Contract amendments audit

1. Introduction

This document summarizes Look4App's Solidity code review on the Smart-Contracts after amendments. We reviewed the following github repository https://github.com/EthWorks/AllSporter-TGE. The changes were made from commits '4d12f291b40cd38151be48b083655ba4d09c7670' to 'ecd3247a8fae86d088dc096ae6fdff759d3b5a6d'. We have approved all of them.

2. Amendments

- Original issue:

  Take a closer look at the *initStates()* function from Tge.sol contract, specifically where *etherCaps* field is set. The *etherCaps* mapping field in Tge.sol contract should store incremental ether caps for specific ICO states for example:
  etherCaps = [0, 10, 20, 30, 40 … 90] which means 10 ether should be collected up to State.PreIco1, 20 ether in total should be collected up to the next state and so on. For the *State.Break* which is the fourth value, the Tge contract stores 0 so the array looks like: [0, 10, 20, 0, 10, 20, 30…].
  This is a bug since starting from the fifth value (10), the values should be higher. Consider this scenario:

deployToken(saleEtherCap = 80, singleStateEtherCap = 10);

deployTge();

initializeTge();

moveState(0, 5);

mint(65)

let currentState = getState()

assert(currentState == State.ICO4)

In the above pseudo-code test, the saleEtherCap is 80, but after receiving 65 ether, the TGE moves to *State.ICOFinished*, which shouldn't happen. The correct state is *State.ICO4.*

✓ Solved:

The ether caps for each ICO stage is now safely set directly from *singleStateEtherCap* field, not by relying on previous ether cap as it was before.

```
etherCaps[uint(State.Preico1)] = singleStateEtherCap;
etherCaps[uint(State.Preico2)] = singleStateEtherCap.mul(2);
etherCaps[uint(State.Ico1)] = singleStateEtherCap.mul(3);
etherCaps[uint(State.Ico2)] = singleStateEtherCap.mul(4);
etherCaps[uint(State.Ico3)] = singleStateEtherCap.mul(5);
etherCaps[uint(State.Ico4)] = singleStateEtherCap.mul(6);
etherCaps[uint(State.Ico5)] = singleStateEtherCap.mul(7);
etherCaps[uint(State.Ico6)] = singleStateEtherCap.mul(8);
```

- Original issue:

  All of the contracts require version 0.4.19 of Solidity. Consider changing the solidity version pragma to the latest version (pragma solidity ^0.4.26;) to enforce latest compiler version.

✓ Solved

- Original issue:

  Constant values can be declared as constant state variables and initialized in the declaration itself (as opposed to in the constructor). Consider doing this for all variables which are initialized in-line e.g. COMMUNITY_PERCENTAGE, ADVISORS_PERCENTAGE etc. in the Allocator.sol contract.

✓ Solved

- Original issue:

  The parameter *totalEtherContributions* in *updateStateBasedOnContributions* function inside the Tge.sol contract is unnecessary. The value *confirmedSaleEther.add(reservedSaleEther)* can be taken directly from the contract.

✓ Solved

- Original issue:

  Remove duplicate imports of ./Minter.sol. In several files, e.g Allocator.sol it's imported twice.

✓ Solved.

core auditor: Michael Frysztacki

LOOK4APP