Genesis Smart Contract Preliminary Audit Report

Project Synopsis

Project Name	**MahaDao Audit**
Platform	Ethereum, Solidity
Github Repo	https://github.com/MahaDAO/arthcoin-v2/blob/develop/contracts/Genesis/Genesis.sol
Deployed Contract	Not Deployed
Total Duration	15 Days
Timeline of Audit	**15th April 2021 to 02nd April 2021**

Contract Details

Total Contract(s)	1
Name of Contract(s)	Genesis
Language	Solidity
Commit Hash	`95fac3e9dca2af67c974f2f87c2c385c4bc03df2`

Contract Vulnerabilities Synopsis

Issues	Open Issues	Closed Issues
Critical Severity	1	0
Medium Severity	1	0
Low Severity	2	0
Informational	2	0
Total Found	6	0

Detailed Results

The contract has gone through several stages of the audit procedure that includes structural analysis, automated testing, manual code review, etc.

All the issues have been explained and discussed in detail below. Along with the explanation of the issue found during the audit, the recommended way to overcome the issue or improve the code quality has also been mentioned.

A. Contract Name: ArthPool

High Severity Issues

A.1 Zero Maha Token amount is minted while calling *_redeemARTHAndMAHA* function

Line no - 314

Description:

As per the current design of the ***_redeemARTHandMAHA*** function, the Genesis token is being burnt while the ARTH and MAHA token is to be minted and transferred to the user.

However, the function does not seem to be adequate as it mints ZERO MAHA tokens every time it is called. This will lead to an unwanted scenario where no MAHA Token is ever minted.

```
306     function _redeemARTHAndMAHA(uint256 amount) internal hasEnded {
307         require(balanceOf(msg.sender) >= amount, 'Genesis: balance < ar
308
309         _burn(msg.sender, amount);
310         _ARTH.poolMint(msg.sender, amount);
311
312         // TODO: distribute MAHA.
313         // HOW?
314         uint256 mahaAmount = 0;
315
316         // NOTE: need to be given and revoked MINTER ROLE accordingly.
317          MAHA.mint(msg.sender, mahaAmount);
```

Recommendation:

The distribution mechanism of MAHA tokens in the **redeemARTHAndMAHA function,** should be implemented in the function body to avoid ZERO tokens being minted.

Medium Severity Issues

A.2 Modifier *hasStarted* never used in the Genesis Contract

Line no - 70

Description:

The Genesis contract includes the ***hasStarted*** modifier at Line 70 but never uses it throughout the contract.

```
70      modifier hasStarted() {
71          require(block.timestamp >= startTime, 'Genesis: not started');
72          _;
73      }
```

While this consumes additional space in the contract, it also adversely affects the gas optimization as well as the readability of the smart contract code.

Recommendation:

Adequate use of all State Variable, modifiers, mappings etc must be ensured in the contract. If the ***hasStarted*** modifier holds no significance it should be removed from the contract.

Low Severity Issues

A.3 Absence of Zero Address Validation

Line no- 124, 139, 146, 153

Description:

The Genesis Contract includes quite a few functions that updates some of the imperative addresses in the contract like ***arthWETHPoolAddres, arthETHPairAddress etc***.

However, during the automated testing of the contact it was found that no Zero Address Validation is implemented on the following functions while updating the address state variables of the contract:

- ***setPoolAndPairs***
- ***setARTHWETHPoolAddress***
- ***setARTHETHPairAddress***
- ***setARTHXETHPairAddress***

Recommendation:

A **require** statement should be included in such functions to ensure no zero address is passed in the arguments.

A.4 External Visibility should be preferred

Explanation:

Those functions that are never called throughout the contract should be marked as ***external*** visibility instead of ***public*** visibility.

This will effectively result in Gas Optimization as well.

Therefore, the following function must be marked as **external** within the contract:

- ***mint #Line 178***
- ***redeem #Line 194***
- ***distribute #Line 203***
- ***getIsRaisedBetweenCaps #Line 219***

Recommendation:
If the PUBLIC visibility of the above-mentioned functions is not intended, then the EXTERNAL Visibility keyword should be preferred.

Informational

A.5 Coding Style Issues in the Contract

Explanation:
Code readability of a Smart Contract is largely influenced by the Coding Style issues and in some specific scenarios may lead to bugs in the future.

During the automated testing, it was found that the Genesis contract had quite a few code style issues.

```
Parameter Genesis.setDuration(uint256)._duration (contracts/Genesis/FLAT_Genesis.sol#1592) is not in mixedCase
Parameter Genesis.setPoolAndPairs(address,address,address)._arthETHPool (contracts/Genesis/FLAT_Genesis.sol#1597) is not in mixedCase
Parameter Genesis.setPoolAndPairs(address,address,address)._arthETHPair (contracts/Genesis/FLAT_Genesis.sol#1598) is not in mixedCase
Parameter Genesis.setPoolAndPairs(address,address,address)._arthxETHPair (contracts/Genesis/FLAT_Genesis.sol#1599) is not in mixedCase
Parameter Genesis.setCaps(uint256,uint256)._softCap (contracts/Genesis/FLAT_Genesis.sol#1606) is not in mixedCase
Parameter Genesis.setCaps(uint256,uint256)._hardCap (contracts/Genesis/FLAT_Genesis.sol#1606) is not in mixedCase
Variable Genesis._WETH (contracts/Genesis/FLAT_Genesis.sol#1496) is not in mixedCase
Variable Genesis._ARTH (contracts/Genesis/FLAT_Genesis.sol#1497) is not in mixedCase
Variable Genesis._ARTHX (contracts/Genesis/FLAT_Genesis.sol#1498) is not in mixedCase
Variable Genesis._CURVE (contracts/Genesis/FLAT_Genesis.sol#1499) is not in mixedCase
Variable Genesis._MAHA (contracts/Genesis/FLAT_Genesis.sol#1500) is not in mixedCase
Variable Genesis._ROUTER (contracts/Genesis/FLAT_Genesis.sol#1501) is not in mixedCase
```

Recommendation:

Therefore, it is highly recommended to fix the issues like naming convention, indentation, and code layout issues in a smart contract.

A.6 NatSpec Annotations must be included

Description:
The smart contracts do not include the NatSpec annotations adequately.

Recommendation:
Cover by NatSpec all Contract methods.

AutoMated Test Results

```
Genesis.setPoolAndPairs(address,address,address)._arthETHPool (contracts/Genesis/FLAT_Genesis.sol#1597) lacks a zero-check on :
        - arthWETHPoolAddres = _arthETHPool (contracts/Genesis/FLAT_Genesis.sol#1601)
Genesis.setPoolAndPairs(address,address,address)._arthETHPair (contracts/Genesis/FLAT_Genesis.sol#1598) lacks a zero-check on :
        - arthETHPairAddress = _arthETHPair (contracts/Genesis/FLAT_Genesis.sol#1602)
Genesis.setPoolAndPairs(address,address,address)._arthxETHPair (contracts/Genesis/FLAT_Genesis.sol#1599) lacks a zero-check on
        - arthxETHPairAddress = _arthxETHPair (contracts/Genesis/FLAT_Genesis.sol#1603)
Genesis.setARTHWETHPoolAddress(address).poolAddress (contracts/Genesis/FLAT_Genesis.sol#1611) lacks a zero-check on :
        - arthWETHPoolAddres = poolAddress (contracts/Genesis/FLAT_Genesis.sol#1615)
Genesis.setARTHETHPairAddress(address).pairAddress (contracts/Genesis/FLAT_Genesis.sol#1618) lacks a zero-check on :
        - arthETHPairAddress = pairAddress (contracts/Genesis/FLAT_Genesis.sol#1622)
Genesis.setARTHXETHPairAddress(address).pairAddress (contracts/Genesis/FLAT_Genesis.sol#1625) lacks a zero-check on :
        - arthxETHPairAddress = pairAddress (contracts/Genesis/FLAT_Genesis.sol#1629)
```

```
Parameter Genesis.setDuration(uint256)._duration (contracts/Genesis/FLAT_Genesis.sol#1592) is not in mixedCase
Parameter Genesis.setPoolAndPairs(address,address,address)._arthETHPool (contracts/Genesis/FLAT_Genesis.sol#1597) is not in mixedCase
Parameter Genesis.setPoolAndPairs(address,address,address)._arthETHPair (contracts/Genesis/FLAT_Genesis.sol#1598) is not in mixedCase
Parameter Genesis.setPoolAndPairs(address,address,address)._arthxETHPair (contracts/Genesis/FLAT_Genesis.sol#1599) is not in mixedCase
Parameter Genesis.setCaps(uint256,uint256)._softCap (contracts/Genesis/FLAT_Genesis.sol#1606) is not in mixedCase
Parameter Genesis.setCaps(uint256,uint256)._hardCap (contracts/Genesis/FLAT_Genesis.sol#1606) is not in mixedCase
Variable Genesis._WETH (contracts/Genesis/FLAT_Genesis.sol#1496) is not in mixedCase
Variable Genesis._ARTH (contracts/Genesis/FLAT_Genesis.sol#1497) is not in mixedCase
Variable Genesis._ARTHX (contracts/Genesis/FLAT_Genesis.sol#1498) is not in mixedCase
```

```
        - Ownable.transferOwnership(address) (contracts/Genesis/FLAT_Genesis.sol#1218-1225)
mint(uint256) should be declared external:
        - Genesis.mint(uint256) (contracts/Genesis/FLAT_Genesis.sol#1650-1664)
redeem(uint256) should be declared external:
        - Genesis.redeem(uint256) (contracts/Genesis/FLAT_Genesis.sol#1666-1673)
distribute() should be declared external:
        - Genesis.distribute() (contracts/Genesis/FLAT_Genesis.sol#1675-1685)
getIsRaisedBelowSoftCap() should be declared external:
        - Genesis.getIsRaisedBelowSoftCap() (contracts/Genesis/FLAT_Genesis.sol#1687-1689)
getIsRaisedBetweenCaps() should be declared external:
        - Genesis.getIsRaisedBetweenCaps() (contracts/Genesis/FLAT_Genesis.sol#1691-1694)
getPercentRaised() should be declared external:
        - Genesis.getPercentRaised() (contracts/Genesis/FLAT_Genesis.sol#1696-1698)
```