OCEANICO.IO

epigenCare

SMART CONTRACTS EXPERTISE — RIGHT WAY TO SUCCESS

EpigenCare Smart Contract Audit

If you have any questions concerning smart contract design and audit, feel free to contact zoia@oceanico.io

Content

Description of the complex of procedures for auditing a smart contract

1. Primary architecture review

- Checking the architecture of the contract.
- The correctness of the code.
- Checking for linearity, shortness, and self-documentation.
- Static verification and code analysis for validity and the presence of syntactic errors.

2. Comparison of requirements and implementation

- Checking the code of the smart contract for compliance with the requirements of the customer code logic, writing algorithms, matching the initial constant values.
- Identification of potential vulnerabilities

Terms of Reference for the creation of a smart contract

- Name of the token - EpigenCare token
- Token Symbol - EPIC.
- Total supply - 60,000,000 EPIC.
- Crowdsale supply - 50,000,000 EPIC.
- Minimum investment - 0.5 ETH.
- Investment rate is 1 ETH to 2500 EPIC.
- The Rate can be changed at the discretion of the company if ETH rate swings too dramatically (unofficially >20% rate change situation).
- The Token cannot be transferred until June 10, 2019, due to SEC holding restrictions.
- One unrestricted transfer is allowed for custodial purposes until August 1, 2018.
- The Token contains a SEC restricted security warning message in code.
- Holding period expiration date can be changed (such as to unlock earlier) if required by law.
- Transfers can be requested and authorized during the restricted period through whitelisting (if requested to the company with proper KYC of recipient address).

List of audited files

Github:

https://github.com/EpigenCare/Crowdsale

The experts conducted an audit of 2 .sol files on the list:

- EpigenCareCrowdsale.sol
- EpigenCareToken.sol

Review of smart contract #1

EpigenCare smart contract review #1

https://github.com/EpigenCare/Crowdsale

Important

1. We recommend you update the pragma solidity to the current version.

2. The name of the token does not match what is stated in the ToR. Should be EpigenCare token instead of EPIC Token

3. We recommend optimizing the requestTokens function for the gas used. Before the if statement, we add the weiPending with weiAmount, and then subtract it in the if block. It is necessary to make an addition in the else block, this will allow not to perform unnecessary actions.

Code quality

1. The code should be as flexible as possible. If you have to change the decimals of the token, then it's already impossible to use ether in totalSupply. It can be accidentally forgotten about this change. We recommend multiplying by 10 ** decimals or creating a constant DECIMALS_MULTIPLIER = 10 ** decimals and multiplying it.

2. All functions using canTransfer can be improved:

   a. The canTransfer function can be replaced with a modifier

   b. Do not copy the source code (transfer, transferFrom), instead use super.transfer (super.transferFrom)

   c. As a result, the transfer method will look like this (transferFrom similarly):

```
function transfer(address _to, uint256 _value)
  public
  canTransfer(msg.sender, _to)
  returns (bool)
{
  return super.transfer(_to, _value);
}
```

3. From the name of the variable openTransfers, it is not obvious what it stores. We recommend you rename it to openTransfersDate / openTransfersTime / openTransfersTimestamp.

Results of contract audit

https://github.com/theabyssportal/DAICO-Smart-Contract

The information in this report is a list of recommendations that need to be followed to ensure the quality and safety of the smart contract.

The experts audited the contract. Based on the results, the developers of the smart contract were given recommendations for improving the optimization of the smart contract code.

Before the deploy Crowdsale contract, we recommend that you remove the remarks mentioned in the “Important” section.

For all questions regarding the audit and testing of the smart contract, we recommend contacting zoia@oceanico.io