Report on the Audit of the code for the Seratio ICO

Sandblocks
Consulting

Author

Dr M.G *Vigliotti*

Tel: +447905320581

Distribution

Prof. O. *Ta'eed*
D. *Kamiski De Sousa*
B. *Mellish*
M. T*aghiyeva*

Centre for Citizenship Enterprise and Governance (CCEG)

SUMMARY

Seratio (www.seratio.com), the commercial enterprise of the Centre for Citizenship Enterprise and Governance (CCEG), has planned, on September 15 2017, an Initial Coin Offering (ICO) for the SeratioCoin. The code has been written and tested by the IT team at Seratio, and Sandblocks Consulting has performed an audit on the code. This document describes the findings of the audit.

Table of Contents

1 Introduction and scope of work

2 Code

The main focus of this report are two contracts:

2.1 SeratioCoin
2.2 SeratioICO
2.3 Security requirements

3 Methodology

4 Results and recommendations

1 Introduction and scope of work

We have been asked to audit the smart contract for the SeratioICO to provide a second opinion of the code and its functional and security properties. The purpose of the audit is to ensure that the code written to manage the Seratio ICO securely implements the requirements contained in the Seratio Whitepaper version 6.0.

In Section "Results and recommendations" we provide in a table form the results of the audit and the recommendations on how to mitigate risk. The cells of the table marked intense red indicate a high level of risk with respect to the cell marked with lighter version of red or yellow.

2 Code

An *Initial Coin Offering* (ICO) marks the creation of a new *coin*. An ICO is similar to a classic IPO (Initial Public Offering), but instead of stocks in a company, buyers get tokens/coins in an online platform.

Seratio will mint and issue the SeratioCoins on the Ethereum platform and sell them to investors/buyers.

I have obtained the code from the IT team at CCEG, and followed the instructions to use the OpenZeppelin and Truffle for compilation a testing purposes.

The main focus of this report are two contracts:

1) SerationCoins (seartiocoin.sol) – the contract creates and assigns properties to the new coin; it enables safe and secure transactions of the coin.
2) SeratioICO (Seratio.ico) – the contract should implement the business logic presented in the Seratio Whitepaper version 6.0; the paper described how the funds will be raised and what proportion of the funds will be used for the development of the Seratio Platform.

   Both contracts are written in Solidity, which is the programming language of the Ethereum platform. Ethereum is a compiled language. Similar to Java, the compilation to binary goes through an intermediate virtual machine called the Ethereum Virtual Machine (EVM). The EVM machine language can be compiled to binaries to run on the Ethereum Blockchain.

2.1 SeratioCoin

The code for the SeratioCoin is meant to create a new coin/token that will be exchanged on the Ethereum platform.

A token requirements are the following:

- A SeratioCoin should be minted from the Seratio's Ethereum address only
- A token can be associated to one address i.e. can have only one owner
- Only the owner of the token should be able to change the ownership of the token.

- A token should be transferable i.e. owners of token should be able to transfer tokens to other addresses/users of their choice

2.2 SeratioICO

The code for the SeratioCoin implements the business logic described in the Seratio Whitepaper version 6.0. Below, we have spelled out the requirements:

- The Seratio will mint SeratioCoins as a token on Ethereum Blockchain
- The Seratio ICO will last for 45 days i.e. buyers have a 45 days window to buy SeratioCoin.
- During the fundraising, the price of the coins, expressed in UK pounds (£) is a function of time. There are two fundraising periods an ***pre-funding 15-day period*** when coins are sold at discounted price
    - £ 0.10 for the first 3 days
    - £0.12 for the 3rd, 4th and 5th day
    - £0.14 for the 6th, the 7th and 8th day
    - £0.16 for the 9th, the 10th and 11th day
    - £0.18 for the 12th, the 13thand 15th day

  and a subsequent **30-day funding period** when coins are sold to the price of £ 0.20 (i.e. from the 16th until the 45th day)

    - The **maximum** amount of investment during the ***pre-funding 15-day period*** is limited to £100 0000. The **maximum** number of coins that could be minted in this period is 10 000 000 (if a £1 000 000 is raised in the first 3 days of pre-funding). The **minimum** number of coins that could be minted in this period is 5 555 555.5555555 (if a £1,000,000 is raised during the 12th, the 13thand 15th day of pre-funding).
    - If an investor is prepared to spend a minimum of £5000 during the pre-funding period, and **maximum** amount of investment allowed (£100 0000) has not been reached, then the buyer is entitled to the discount associated to the pre-funding period.
    - If an investor is prepared to spend a minimum of £1000 during the funding period then buyer is entitled to buy the SeratioCoin for the price of £0.20.
    - The total supply of SeratioCoins has not been fixed
    - The campaign has not set a minimum capital of money to raise i.e. no money needs to return to investors
    - The campaign pledges to spend only £ 5 000 000 for the Seratio platform out of the total amount capital raised. The excess of capital will use by CCEG.
    - No exchange rate between SeratioCoin and Ether has been fixed

- The Ether account where the money will sent is going to be published on the following website http://seratio-coins.world

2.3 Security requirements

To ensure the fairness of the system for the users, we add the two requirements below:

1. A buyer that pays the minimum amount during the ICO funding will be entitled to a total amount of SeratioCoins when the ICO is completed. For example, if a buyer pays £ 1000 in the 44th day of the funding campaign then the buyer will receive SER 5000 when the ICO is completed.
2. A buyer will not be able to receive any SeratioCoin, i.e. the transaction will be void, if the user sends the wrong amount of money. For example a user sending £ 4990 on the 10th day of the campaign will not receive any SeratioCoin and the Ether will return to the buyer.

   From a security point of view, attackers should not be able to:

3. Acquire, or transfer or token/SeratioCoin, unless the attacker owns the coins
4. Create new SeratioCoins
5. Violate any of the requirements (informally) described in Sections 2.1 and 2.2.

The SeratioICO works as follows:

- Buyers will decide on an amount of money and a time to invest consistently with the requirements in Sections 2.1 and 2.2
- Buyers will purchase an equivalent amount of Ether and send to the Ether Address of the Seratio
- When the ICO is completed, the total amount of SeratioCoins will be determined and it will be distributed by Seratio to the addresses of the owners of the SeratioCoins.

3 Methodology

We have manually reviewed the source code to ensure that: the requirements described in Section 2.1 and Section 2.2 are satisfied, and that the code is free from well-known security bugs.

4 Results and recommendations

Compilation of code
The code uses the libraries from OpenZeppelin. These have been updated on July 02,2017. OpenZeppelin v 1.0.5 that supports the compilation of the code – see https://github.com/OpenZeppelin/zeppelin-solidity/releases

In the future, if OpenZeppelin v 1.0.5 will be used the command "`install zeppelin@1.0.5`" should be deployed.

Code for the SeratioCoin

The code is simple, clear, modular and elegant. The OpenZeppelin library guarantees that the functional requirements for the Seratiocoin (see Section 2.1) hold. The OpenZeppelin library also follows best practice in preventing the introduction of software bugs that could have adverse impact on the code.

The only file that could be exposed to attacks is "StandardToken.sol"; the code does not prevent a race condition that could lead to an unauthorised transfer of Ether- see https://github.com/ethereum/EIPs/issues/20 - issuecomment-263524729

Recommendation- Move to OpenZeppelin v 1.2.0, i.e. the most recent update (it will require to update the "SeratioICO.sol " import of the "SafeMath.sol")

SeratioICO

The code for the Seratio CO did not pass the last two tests devised by CEEG IT team - the output from Truffle is reported below

```
1) Should respect investment cap for phase one
> No events were emitted
2) Should create right amount of tokens for Seratio
> No events were emitted
```

Recommendation-Investigate why these tests and ensure that all the all tests are passed

Code documentation

If the code were extensively documented, it would be easier for third parties to understand it. Specific comments on the code are included in the document attached – SeratioICO_SC.sol

Recommendation -Address all issues highlighted by the comments – see

"/*SC: "Comment from Sandblock Consulting "*/

Business logic

Part of business logic described in the white paper seems missing from the code. During the pre-funding period only the equivalent of £ 1000 000 of SeratioCoin can be bought at a discounted price. *The code that checks condition hold does not appear in the file provided to me.* Assuming that the ICO is very successful and that £ 1000 000 is reached before the end of the prefunding period, then it is underspecified in the white paper on the consequences of this state of affairs. There are two ways forward:

1. Investors are allowed to buy SeratioCoins at the price of £ 0.20 during the pre-funding period **or**
2. Investors have to wait for the pre-funding period to end

Recommendation -Implement the first solution in the Seratio smart contract, and calrify this position in the white paper. The second option, selling undiscounted SeratioCoins in a pre-funding period, underminses the purpose of having a pre-funding period.

Exchange rate ETH/£

The white paper sets the price for the SeratioCoin in British pounds (£). The investors will buy the SeratioCoins in Ether. To determine the right amount of SeratioCoins investors are entitled, the conversion Ether/Pounds needs to be performed. The price of Ether can have substantial fluctuations during the course of a day, and it seems that fixing the exchange rate Ether/Pounds as currently done in the code could lead to investors receiving fewer (or more) tokens than expected.

Recommendation -Contract on the blockchain cannot be changed; hence the contract cannot closely follow the price of Ether.

As the minting of the SeratioCoins happens when the ICO is completed, the correct amount of British pounds can be accurately computed from the timestamp of the transaction associated with the purchase of the token.

Web-security

Information related to the ICO will be held on webpage http://seratio-coins.world. An adverse impact on the ICO can be delivered if this webpage is compromised – see the attack on CoinDash which led to a loss of $7 million https://www.bleepingcomputer.com/news/security/hacker-steals-7-million-worth-of-ethereum-from-coindash-platform/

Recommendation Host the webpage http://seratio-coins.worldon Cloudflare https://www.cloudflare.com/plans/pro/ - or similar services

Couldflare would provide Seratio with a Firewall, and it guarantees that:

- The domain name will not get spoofed,
- Protection from Cross Site Scripting Attacks (i.e. protection from the attack that led to CoinDash' loss of money) and DDoS attacks

White paper

The Seratio Whitepaper 6.0 contains a few typos, information is duplicated, and the general structure of the paper could be simplified and provide more clarity to the reader. This could have a positive impact the fundraising.

Recommendation – Address the comments in the documented attached

Consider the statement at page 9 that suggests that the total number of SeratioCoins minted would 25 000000 in case of an investment of £ 5000 000". If an investment of £ 5000 000 is raised during the ICO, then the amounts of SeratioCoins minted would be between 30 000 000 and 25 555555.5555555.

The information regarding the "Due Diligence team " is repeated three times. We recommend putting in the paper twice- in the Executive Summary and later on when presenting the team.