GiveCoin ERC223 Token Audit - INCOMPLETE
September 27, 2017
Raine Revere
raine@maiden.global

*This audit was paused as requested by the Grant Hero Foundation due to anticipated shortage of funds and should not be considered ready for publication.

Overview

A partial security audit of the GiveCoin ERC223 Token was performed by Raine Revere of Maiden Global at commit hash `4c9ba8341122b8ad87f28578f0e57d4340519df2` in github.com/granthero/givecoin (backup at rgithub.com/maidenglobal/audits/tree/master/givecoin). A copy of this report can be found at github.com/maidenglobal/audits/tree/master/givecoin/givecoin.pdf.

Audit

Token Description
The GiveCoin token contract conforms to the Ethereum ERC223 interface.

Name: GiveCoin (at time of audit)
Symbol: GC (at time of audit)
Total supply: 50,000,000
Decimals: 2 (at time of audit)

Audit Notes

- Ownable ✓
- SafeMath ✓
    - Min/Max functions not used
- token_database
    - configure
        - ✗ Can be modified after creation
    - total_supply is fixed
    - variables
        - ✗ Recommend removing unused values or stored as bytes32 which can be returned
- token
    - Notes
        - token_database contained
    - transfer1 ✓
    - transfer2 ✓
    - donate
        - ✗ donor and recipient are not verified
        - ✗ call with 0 many times?
            - Recommend if statement to check for 0 value
    - configure
        - ✗ Can be modified after creation
    - Burn
        - ✗ remove
- ico
    - CHECKLIST
        - access control
        - payable ✓
        - sends
        - overflow/underflow
        - roles
        - address payload
        - array push
        - reentry
    - Notes
        - token contained
        - withdrawal_address is creator
        - Duration
            - 28 days after creation
            - 300 GC/ETH
        - start_timestamp marks beginning of ICO
    - configure
        - ✗ Can be modified after creation
    - fallback
        - only fallback is payable
        - Min contribution is 0.01 ETH

        - Recommend use ether keyword instead of 10**18
        - ✗ uint256 reward = GiveCoins_per_ETH.mul(msg.value) / 10**18;
            - limited by MAX_WEI / 30000
        - Buy _tokens = tokens remaining
        - ✗ SafeMath not used
        - ✗ withdrawal_address.send(this.balance);
            - return value is not checked—but this is okay since they can withdraw later
            - will fail if withdrawal_address is incorrect (which can be changed)
            - tokens will still be transferred
        - participants pay the gas for every withdraw
    - ✗ adjust_price
    - ✗ change_end_timestamp
    - ✗ change_withdrawal_address
    - ✗ closeICO can be called prematurely
    - withdraw_tokens
        - ✗ transfers to owner instead of withdrawal_address
        - ✗ withdrawal_address is same as owner
    - ✓ mutex
- Questions
    - Are the debugging functions intended to be included in the final version?

Extra-Audit Concerns

Auditor Disclosure

Audit payment is in USD payable 30 days after the token sale contingent upon no newly reported or exploited major vulnerabilities. This is to incentivize the auditor to perform the highest quality audit.

Non-Endorsement

Statements in the final report do not imply an endorsement or recommendation of the utility or economic value of SALT tokens or smart contracts that use the tokens, partnership with Salt Lending beyond the audit, an advisor relationship, or endorsement of Salt Lending's business model or activities beyond the security of the audited smart contracts.