SOLIDIFIED

Audit Report for Cycled ICO. April 5, 2018.

Summary

Audit Report prepared by Solidified for Akeo covering the Cycled token, crowdsale and whitelist contracts.

Process and Delivery

Four (4) independent Solidified experts performed an unbiased and isolated audit of the below token sale. The debrief took place on April 5, 2018 and the final results are presented here.

Audited Files

The following files were covered during the audit:

- CycledToken.sol
- CycledCrowdsale.sol
- Whitelist.sol

Notes

The audit was conducted on commit `79b8ebfd051434ae280afbc707452c0b7a15a5f5`
The audit was based on the solidity compiler `0.4.19+commit.c4cbbb05`

Intended Behavior

The purpose of these contracts is to create the Cycled token and distribute it to the public, in a crowdsale process.

Issues Found

1. Contract is not trustless

A lot of the contracts' core functionalities rely heavily on the owner's action and, although some of them are considered out of scope, they still incur high risk for the users. This list of risks includes but is not limited to:

- not respecting the soft cap
- not returning overpaid ETH
- not burning remaining tokens
- pausing and unpausing the token at will.

Recommendation
Reconsider the role of the owner, taking into consideration the context of smart contracts and the trustless nature that they carry. As it stands, the contract cannot be considered secure for users, as a lot of failures can happen during the purchase process.

AMENDED [25.04.2018]
A series of actions were taken to mitigate this issue, which include a soft cap mechanism, together with a refund system and an automatic burning at the end. The contracts can now be considered mostly trustless. Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

2. Owners of the crowdsale can provide discounts/special deals for 3rd parties privately

---

Buys executed by the owner with `issueTokens` are not immediately distinguishable from those purchased through the mechanics of the crowdsale. Also, owner of the token contracts has the ability to transfer tokens, approve transfers and revoke the approval from the crowdsale contract at any moment from the creation of the contract, making possible to negotiate tokens outside of the crowdsale contract. In the event of suspected fraud, it would be difficult to prove that the buy occured within the terms of the crowdsale.

Recommendation
Only allowing purchases in Ether reduces the complexity of
- ensuring the trustlessness of the sale mechanics
- calculating refunds
and should be considered strongly.

AMENDED [25.04.2018]
`IssueTokens` function has been removed and now only ETH purchases are accepted. Fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

3. Multiple contract versions in the same codebase

The contracts rely on an outdated version (1.5.0) of the Open Zeppelin framework to manage ERC20 standard functions. The current version is 1.8.0. The flat file included in the project uses different versions of the library for functions (1.8.0/1.6.0). The CycledCrowdsale and Whitelist contracts are also different and seem to be outdated in the flat file.

Recommendation
Along with encouraging the continued use of Open Zeppelin, we recommend that the codebase is updated to the latest stable version, as any bugs and vulnerabilities found by the community should be patched in recent versions.

AMENDED[25.04.2018]
Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

4. Early buyers can resell tokens during the sale

An early buyer (in the first or second discount cap) can resell their tokens during the main sale at a cheaper price than the CycledCrowdsale offers. It is also possible to resell it to non-whitelisted addresses. It all can be done in a trustless manner if the early buyer provides a contract address during the whitelist process.

Recommendation
If resale during the presale is not desired, consider implementing a transfer constraint in the token contract. Beware that the crowdsale still needs to be able to transfer tokens to complete purchases.

AMENDED[25.04.2018]
Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

5. Update Compiler Version

We recommend using the latest stable compiler version, which is 0.4.21 as of this writing.

AMENDED [25.04.2018]
Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

6. Contract `Whitelist` is gas inefficient

The whitelist does not have the ability to add/remove whitelisted addresses in batches, so each whitelisted address adds overhead of a new transaction.

Recommendation
Consider using OpenZeppelin's whitelist implementation which has batch adding/removing feature.

AMENDED [25.04.2018]
Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

7. Lack of input validation

Input is not validated in the following places:

- Constructor of CycleToken.sol

Invalid inputs could lead the contract to unintended behavior. In the examples above, for instance, null addresses could be used in the place of wallets, which if uncaught would result in the loss of tokens.

Recommendation
We recommend that validation is performed for all inputs.

AMENDED [25.04.2018]
Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

8. Sale still accepts bids when cap is reached

Consider implementing a mechanism that puts the sale in a closed state after the cap is reached. Otherwise it would still accept transactions and fail later on the buying process, incurring more gas expenses to buyers.

AMENDED [25.04.2018]
Issue fixed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

9. Consider using OpenZeppelin's RefundableCrowdsale

We recommend building CycledCrowdsale on top of OpenZeppelin's RefundableCrowdsale, or integrating their RefundVault. This will both mitigate some of the trust issues mentioned in 1 as well as add the finalization state recommended in 8.

AMENDED [25.04.2018]
RefundableCrowdsale and RefundVault were implemented. FIxed by Akeo team in commit `4612da72313bf1322f88fddc274dd2599bdea632`

Closing Summary

Akeo team has taken measures to address all the issues found with the Cycled crowdsale smart contracts to adhere to the promised behavior.

CycledToken.sol has been verified as fully ERC20 compliant, and has taken recommended measures to mitigate the known EIP20 API Approve / TransferFrom multiple withdrawal attack.

Beyond the issues mentioned, the contracts were also checked for overflow/underflow issues, DoS, and re-entrancy vulnerabilities. None were discovered.

OpenZeppelin contracts such as Ownable/SafeMath/etc. have been widely audited and secured, as such, they were not prioritized for auditing.

Audit Report for Cycled ICO. April 5, 2018.

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of the Cycled platform or its products. This audit does not provide a security or correctness guarantee of the audited smart contracts. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

Solidified Technologies Inc.