# THELEDGER.

## Identify contract audit:

## Presale phase summary

# CONTACT INFO

**TheLedger NV**
Business Park King Square
Veldkant 33B
2550 Kontich
Belgium
Phone: +32 (0)3 871 99 67
VAT: BE0671.584.745

**Contacts**

Thomas Marckx
Co-Founder – TheLedger
thomas.marckx@theledger.be
+32 479 52 61 10

Andries Van Humbeeck
Co-Founder – TheLedger
andries.vanhumbeeck@theledger.be
+32 498 77 70 41

Kevin Leyssens
Blockchain Bandit – TheLedger
kevin.leyssens@theledger.be
+32 491 07 79 58

**“In a gentle way you can shake the world.”**

**- Mahatma Gandhi**

# INDEX

# CONCLUSION

We audited all the contracts in the pre-sale and we deem them as production ready. We do still recommend reviewing the contracts by multiple third parties.

We are aware a possible integer underflow and reentrancy is possible at the “approveAndCall” method in the CustomToken.sol smart contract. But this is not one of a critical kind.

This document is a summary of a complete audit document delivered on Wednesday 16th of May 2018. The hash (checksum of sha-256) of the complete delivered audit document is:

79D90637173EB85609672698B64D9A723D7B9D98CBECB306E1B1EB85D0B01775

# STATIC ANALYSIS RESULT[1]

We ran the codebase through multiple open-source analysis tools to check for well-known bugs, errors and attack vectors.

| Attack vector | Result |
|---|---:|
| EVM Code Coverage[2] | 100% |
| Callstack Depth Attack Vulnerability | False |
| Transaction-Ordering Dependence (TOD) | False |
| Timestamp Dependency | False |
| Re-Entrancy Vulnerability | False |
| Parity multisig bug 2 | False |

[1] Using multiple open source tools like Oyente and Mythril

[2] Number of opcodes executed / total number of opcodes

# TESTED VULNERABILITIES

In the table below, we summed up some well-known vulnerabilities. Divided in 3 levels: Solidity, EVM and blockchain. On the last column a description is of possibility is written down.

| Level | Cause of vulnerability | Possible |
|---|---|---|
| Solidity | Call to the unknown (DAO) | Only in the approveAndCall method. But this has no critical effects. |
| | Gasless send | No. |
| | Exception disorders | Using 'required' keywords to check input parameters. |
| | Type casts | Not applicable. |
| | Reentrancy | In the CustomToken approveandcall method due to the low-level call method. But checks are in place to not harm the contract when this is executed. |
| | Keeping secrets | No secrets are necessary. |

| | | |
|---|---|---|
| EVM | Immutable bugs | Tests are written for finding bugs. Note that there can never be a 100% certainty of bug-free contracts. |
| | Ether/token lost in transfer | Don't send to 'orphan' addresses. Meaning addresses that are not associated to any user or contract. But these tokens can be transferred back by the owner of the token. |
| Blockchain | Unpredictable state | Multiple checks are in place. |
| | Time constraints | Only for begin and end time of presale. But miners can only modify time in a small way. These small modifies have no serious impact on the presale. |

# TESTS

The total code coverage is 96% on functions.[3] Tests are written in JavaScript.

| **Contract** | **#test** |
|---|---:|
| Identify Token | 20 |
| Presale | 24 |
| Whitelist | 19 |
| MultiSig | 22 |
| **Total** | **85** |

[3] Tested with the solidity-coverage tool from sc-forks (https://github.com/sc-forks/solidity-coverage)

# SAFETY FUNCTIONS IMPLEMENTATION

## PAUSE FUNCTION

This function can only be invoked by the owner of the presale. This is a safety function when things go wrong, or a bug is found, the damage will be limited.

## ENABLE TRANSFER FUNCTION

The enable transfer will only be used in the transfer and transferFrom (and functions derived from it) functions. Your contract still works properly, just the transferring of tokens will be enabled or disabled. This can be useful when a malicious person has found a way to extract tokens. Through the enableTransfer this will be stopped. When implementing a burn function, these tokens can be burned.

## ISCONTRACT FUNCTION

Contracts cannot participate in the presale. This choice is obviously made to reduce the attack vector.