ChainSecurity

Security Audit of Cointed Smart Contract

This report is public.

ChainSecurity Ltd.

October 11, 2017

COINTED
THE FUTURE OF MONEY

Contents

Token Name	Cointed Token (CTD)
Decimals	18
Smallest Unit (Atom)	10^{-18}CTD
Token Amount	Up to 650,000,000 CTDs (Section 1.1)
Token Price	Fixed to 1000-1150 CTDs/ETH (Section 1.2)
Percentage for sale	100%
Minimum Token Purchase	1 Wei
Maximum Token Purchase	No Limit
Minimum Funding Goal	None
KYC	None
Refund	Yes, see Section 1.3
Owner Rewards	Yes, see Section 1.2
Extra Features	Pausable, Upgradable, . . . , see Section 1.4

Table 1: Facts about the token and the token sale.

We first and foremost thank Cointed for giving us the opportunity to audit your smart contract code. This documents outlines our methodology, limitations and results for your security audit.

1 System Overview

Cointed provides a platform for a fast and convenient way to exchange cryptocurrencies for fiat money.

In the following we describe their Cointed Token (CTD) and their corresponding token sale. Table 1 gives the general overview.

1.1 Token Amount

The maximum token amount is generally given by the `TOTAL_LIMIT` variable as 650 million CTDs. Tokens are minted during the crowdsale and the total supply is fixed at the end of the crowdsale so that the maximum token amount might not be reached. In case the maximum number should be reached, the crowdsale allows for up to 1,514 atoms to be created due to arithmetic imprecisions.

1.2 ICO Phases

The token sale goes through the following phases:

1. Before the ICO: Allows Cointed to perform contract setup
2. Pre-ICO A: Phase with 15% bonus
3. Pre-ICO B: Optional phase with 10% bonus
4. ICO: Regular ICO Phase
5. After the ICO: No more token purchases are possible (see Section 1.3)

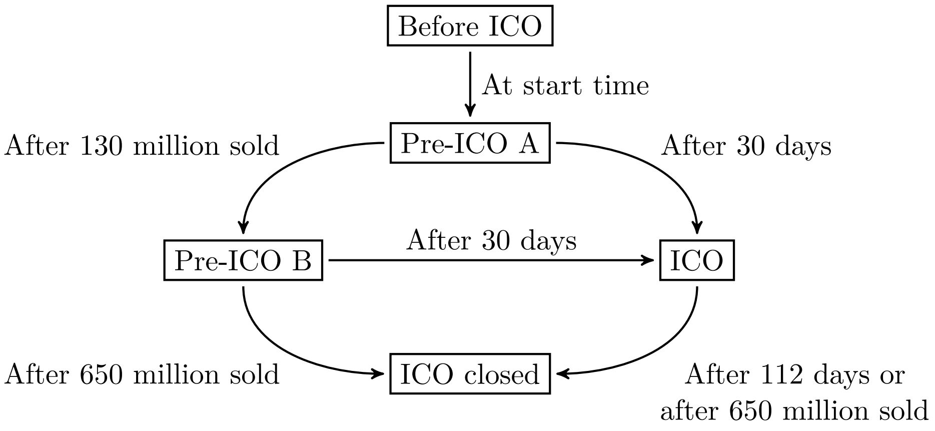

Figure 1: State Transitions for the Crowdsale.

The phase transitions are displayed in Figure 1. They can either happen due to elapsed time or as a certain number of tokens has been purchased.

Token Prices: The token buyer receives the following amount of tokens in the phases per ETH:

Phase	Token Buyer	Owner	Bounty
Pre-ICO A	1150	304	61
Pre-ICO B	1100	292	58
ICO	1000	263	52

As the table shows, with each token purchase additional tokens are minted for the owner and the bounty account.

Phase change rewards: Cointed offers special phase change rewards.

- The first token buyer during the Pre-ICO A phase receives 0.1 ETH
- If the Pre-ICO A phase sells out, the final token buyer receives 0.1 ETH
- If the ICO phase is entered, the first token buyer receives 0.2 ETH
- If the Pre-ICO B phase or the crowdsale is sold out, the last token buyer receives 0.5 ETH

These rewards have to be claimed in the same way as refunds, see Section 1.3. Note, that these rewards only work if Cointed provides the required amount of funding to the contract.

1.3 Refund Options

Refunds can occur in the following situations:

- A token purchase at the end of a phase might get partially refunded for those funds which exceed the phase limit. ⇒ Partial Refund
- An attempted token purchase after the end of the ICO in case the tokens were not sold out. Note, that only the first such token purchase is refunded, while later attempts are blocked using the `whenNotClosed` modifier. ⇒ Full Refund

As the contract has no minimum funding goal, no token purchases can be refunded.

Important: Note, that refunds are not directly send back, but must be withdrawn using the `withdraw` function. Token buyers are notified of a pending withdrawal with the `Withdrawal` event. Furthermore, to protect token buyers after the completion of the ICO, these refunds cannot be accessed by Cointed for 30 days. Afterwards, Cointed has the opportunity to withdraw unclaimed refunds using the `returnWei` function.

1.4 Extra Features

Pausable Cointed has the power to pause the token sale **once** for the duration of two weeks. During this time no token transfers, token purchases or refunds can be made.

Upgradable Cointed can propose a token upgrade to new token version. This can happen at any time. Individual token owners can accept the upgrade by calling the `upgrade` function.

Owner Limits The contract limits the owner's power during the ICO. During the ICO the contract owner cannot transfer any tokens.

Safe Defaults Should Cointed fail to perform a proper setup before the start of the token sale, then the contract will automatically assign its owner to critical functions.

2 Audit Overview

2.1 Scope of the Audit

The audit was based on the Ethereum Virtual Machine (EVM) after `EIP-150` and solidity compiler `0.4.17+commit.bdeb9e52.Linux.g++`.

The scope of the audit is limited to the following source code files. All of these source code file were finally retrieved on October 9th, 2017:

- CtdToken.sol
  - Final SHA-256: `3dc564c3fac6de6bd0c21d437400c489375dc5098353057c2e5ea74730d8f9ef`
- InterfaceUpgradeAgent.sol
  - Final SHA-256: `f3c312a90c3b4d2c4b19d50c171b54917f083f8d0ae446206dd64233600627dc`
- PausableOnce.sol
  - Final SHA-256: `ab900efc07d968b2eba5579f555505205500b7156a5e8cd1622a7a7b42486d2b`
- UpgradableToken.sol
  - Final SHA-256: `2fe1dfeec7fd85c6d071b36c25509fe2e94a3fc86c68640400b555eb3bb7235e`
- Withdrawable.sol
  - Final SHA-256: `cc25f011784254b7e0e9c1dc5667cf5da37ce06d1c1148299fd6ed70b97c37d5`

As most users might check the code through platforms such as etherscan, they see a flattened, single-file version of the code. We also provide the SHA-256 for this flattened code: `e29e8d942dbbec9cf02e5342d22bf0dbc225c70d6586a12f9c6cd93fc84ffb29`.

2.2 Depth of Audit

The scope of the security audit conducted by ChainSecurity Ltd. was restricted to:

- Scan the contracts listed above for generic security issues using automated systems and manually inspect the results.
- 1-day manual audit of the contracts listed above for security issues.

2.3 Terminology

For the purpose of this audit, we adopt the following terminology. For security vulnerabilities, we specify the *likelihood*, *impact* and *severity* (inspired by the OWASP risk rating methodology[1]).

Likelihood represents the likelihood of a security vulnerability to be encountered or exploited in the wild.

Impact specifies the technical and business related consequences of an exploit.

Severity is derived based on the likelihood and the impact calculated previously.

We categorize the findings into 3 distinct categories, depending on their criticality:

- Low - can be considered as less important
- Medium - needs to be considered to be fixed
- High - should be fixed very soon
- Critical - needs to be fixed immediately

During the audit concerns might arise or tools might flag certain security issues. If our careful inspection reveals no security impact, we label it as ✓ No Issue. Finally, if during the course of the audit process, an issue has been addressed technically, we label it as ✓ Fixed, while if it has been addressed otherwise we label it as ✓ Addressed.

Findings that are labelled as either ✓ Fixed or ✓ Addressed are resolved and therefore pose no security threat. Their severity is still listed, but just to give the reader a quick overview what kind of issues were found during the audit.

3 Limitations

Security auditing cannot uncover all existing vulnerabilities, and even an audit in which no vulnerabilities are found is not a guarantee for a secure smart contract. However, auditing allows to discover vulnerabilities that were overlooked during development and areas where additional security measures are necessary.

In most cases, applications are either fully protected against a certain type of attack, or they lack protection against it completely. Some of the issues may affect the entire smart contract application, while some lack protection only in certain areas. We therefore carry out a source code review trying to determine all locations that need to be fixed. Within the customer-determined timeframe, ChainSecurity Ltd. has performed auditing in order to discover as many vulnerabilities as possible.

[1] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

4 Details of the Findings

4.1 No Reentrancies ✓ No Issue

The Cointed contract does not contain any vulnerabilities that would allow reentrancy attacks. This is because no untrusted code is ever invoked.

4.2 No Callstack Bugs ✓ No Issue

The Cointed contract does not contain any vulnerabilities that would allow attacks based on a callstack overflow. This is because all exception are properly handled and propagated.

4.3 Ether Transfers ✓ No Issue

Ether transfer can lead to variety of issues in Ethereum. These issues include callstack bugs, reentrancies and denial-of-service attacks. For Cointed, Ether transfers only occur during `create` and `returnWei` to the trusted owner account and during withdraw where it safely happens at the end of the function. In all cases, Cointed uses the `transfer` function. Thereby, Cointed eliminates callstack bugs during ether transfers.

4.4 Safe Math ✓ No Issue

Cointed also uses the popular `SafeMath` library for critical operations to avoid arithmetic over- or underflows and safeguard against unwanted behaviour.

In particular, critical variables such as `totalSupply`, `balances` and `totalProceeds` are only updated using `SafeMath` operations or constants.

4.5 Possible conflict between owner and buyer refunds Low ✓ Fixed

After the end of the crowdsale, see Section 1.2, the original contract allowed Cointed to use the `returnWei` function to drain all funds from the contract. If the contract gets sold out, it is likely that token purchases arrive after its closing. These are stored as refunds, see Section 1.3. Additionally, the final award will be stored as a withdrawable refund. In theory, Cointed would have had opportunity to immediately retrieve these funds.

Fixed: Cointed introduced a new 30-day delay to fix this issue in the code and make sure that token buyers can withdraw their refunds. This has been implemented through the `afterWithdrawPause` modifier of the `returnWei` function:

Listing 1: returnWei() in CtdToken.sol

```
    function returnWei() onlyOwner whenClosed afterWithdrawPause public {
        owner.transfer(this.balance);
    }
```

Likelihood Low

Impact Low

4.6 Potential misunderstanding about withdrawals Low ✔ Addressed

Most crowdsale contracts immediately refund overspent ether fund to the originator. As described in Section 1.3, Cointed instead stores these refunds as potential withdrawals. If token buyers are unaware of this feature, they might “lose” their funds as they will not withdraw them. Token buyers might also (incorrectly) feel that they have been betrayed, as they would not receive the refund immediately.

Additionally: Cointed has given an assurance that it will make token buyers aware of this functionality and how to withdraw refunds. Also, as described in Section 1.3, Cointed uses `Withdrawal` events to notify token buyers.

Likelihood Low

Impact Low

4.7 Potential transition from Pre-ICO A to Post ICO phase Low ✔ Fixed

As described in Section 1.2, a single, enormous purchase of at least 520 million tokens could lead to a transition from the Pre-ICO A phase straight to the Post-ICO phase. This was not intended by Cointed, but due to its volume, this transfer is unlikely. In the case of such a transfer, intermediate awards would not be paid out.

Fixed: Cointed introduced a fix that correctly handles phase transitions due to purchase goals being reached.

Likelihood Low

Impact Low

5 Conclusion

The COINTED smart contracts have been analyzed under different aspects, with different open-source tools as well as our fully fledge proprietary in-house tool. Overall, we found that COINTED employs good coding practices and has clean, documented code. We have no remaining security concerns about the COINTED smart contracts, as all detected issues were either fixed or addressed.

ChainSecurity

6 Disclaimer

UPON REQUEST BY COINTED, CHAINSECURITY LTD. AGREES MAKING THIS AUDIT REPORT PUBLIC. THE CONTENT OF THIS AUDIT REPORT IS PROVIDED "AS IS", WITHOUT REPRESENTATIONS AND WARRANTIES OF ANY KIND, AND CHAINSECURITY LTD. DISCLAIMS ANY LIABILITY FOR DAMAGE ARISING OUT OF, OR IN CONNECTION WITH, THIS AUDIT REPORT. COPYRIGHT OF THIS REPORT REMAINS WITH CHAINSECURITY LTD..