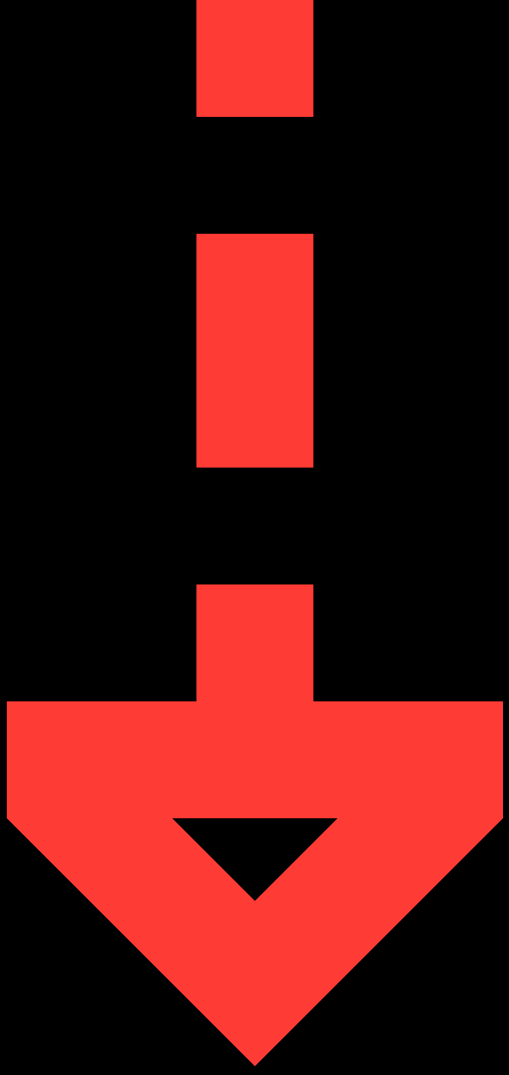
WISE
Contract Audit



REPORT DATE	January 14th, 2019
REPORT VERSION	2.0

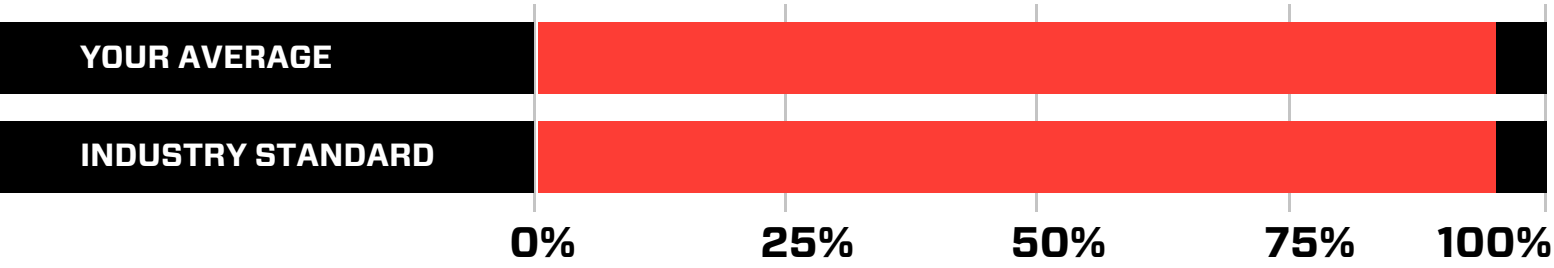
PREPARED BY

This document outlines the overall security of Wise.cr's smart contract as evaluated by Hosho's Smart Contract auditing team. The scope of this audit was to analyze and document Wise.cr's token contract codebase for quality, security, and correctness.

Contract Status

No issues were discovered in this contract during the auditing process. (See Complete Analysis)

Testable Code



Testable code is 94.93%, which is on par with the industry standard of 95%. (See Coverage Report)

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the Ethereum network's fast-paced and rapidly changing environment, we at Hosho recommend that the Wise.cr team put in place a bug bounty program to encourage further and active analysis of the smart contract.

Table of Contents

Auditing Strategy and Techniques Applied

The Hosho team has performed a thorough review of the smart contract code, the latest version as written and updated on January 13th, 2019. All main contract files were reviewed using the following tools and processes. (See All Files Covered)

Throughout the review process, care was taken to ensure that the token contract:

- Implements and adheres to existing ERC-20 Token standards appropriately and effectively;
- Documentation and code comments match logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices in efficient use of gas, without unnecessary waste;
- Uses methods safe from reentrance attacks; and
- Is not affected by the latest vulnerabilities.

The Hosho team has followed best practices and industry-standard techniques to verify the implementation of Wise.cr's token contract. To do so, the code is reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as they are discovered. Part of this work includes writing a unit test suite using the Meadow testing framework. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

1	**Due diligence in assessing the overall code quality of the codebase.**
2	**Cross-comparison with other, similar smart contracts by industry leaders.**
3	**Testing contract logic against common and uncommon attack vectors.**
4	**Thorough, manual review of the codebase, line-by-line.**
5	**Deploying the smart contract to testnet and production networks using multiple client. implementations to run live tests.**

2.1 Summary

The Wise.cr contracts are formed by an ERC-20 token and an ICO crowdsale that will be used to sell the WiseToken. The token contract is based off of a detailed ERC-20 token, with additional functionality added for token minting and pausing capabilities. The crowdsale is a capped and mintable sale that will be conducted in three stages, as well as a timelocked contract to be used for investor token distributions.

2.2 Coverage Report

As part of our work assisting Wise.cr in verifying the correctness of their contract code, our team was responsible for writing a unit test suite using the Meadow testing framework.

- Branches: 92.86%
- Functions: 93.75%
- Lines: 98.18%

2.3 Failing Tests

No failing tests!

For ease of navigation, sections are arranged from most critical to least critical. Issues are tagged “Resolved” or “Unresolved” depending on whether they have been fixed or still need addressing. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

Critical

The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

High

The issue affects the ability of the contract to compile or operate in a significant way.

Medium

The issue affects the ability of the contract to compile or operate in a significant way.

Low

The issue has minimal impact on the contract’s ability to operate.

Informational

The issue has no impact on the contract’s ability to operate, and is meant only as additional information.

3.1 Unused Imported Contract

INFORMATIONAL

Contract: WhitelistedCrowdsale

Explanation

WhitelistedCrowdsale is imported by WiseCrowdsale but is not used in any contract.

Update

The reference to WhitelistedCrowdsale was removed from the WiseCrowdsale contract.

We are grateful to have been given the opportunity to work with the Wise.cr team.

The Wise.cr contracts create a specialized token and crowdsale. The contracts are well written and follow proper ERC-20 Specification. One informational issue discovered during the audit process has been remedied by the Wise.cr team, and all Wise.cr contracts have passed Hosho's auditing process.

The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them.

We at Hosho recommend that the Wise.cr team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

Test Suite Results

Contract: WiseMeadow.OwnableTests

√ transferOwnership_senderIsNonOwner_ExpectRevert (0.0083630s)
√ renounceOwnership_calledByOwner_EmitOwnershipTransferredEvent (0.0347360s)
√ transferOwnership_calledByOwner_EmitOwnershipTransferredEvent (0.0182370s)
√ transferOwnership_newOwnerIsZeroAddress_ExpectRevert (0.0090730s)
√ transferOwnership_calledByOwner_UpdateOwnerVariable (0.0177030s)

Contract: WiseMeadow.PausableTests

√ pause_IsPaused_ExpectRevert (0.0273810s)
√ unpause_IsPaused_EmitUnpausedEvent (0.0300640s)
√ paused_StateIsFalse_UpdatePausedState (0.0052190s)
√ pause_NotPaused_EmitPausedEvent (0.0236040s)
√ unpause_NotPaused_ExpectRevert (0.0076280s)

Contract: WiseMeadow.SafeMathTests

√ RevertSubtractionOverflow (0.0467170s)
√ AllowRegularAddition (0.0028170s)
√ RevertAdditionOverflow (0.0471470s)
√ RevertMultiplyOverflow (0.0751320s)
√ AllowRegularDivision (0.0091810s)
√ SkipOperationMult0 (0.0235170s)
√ AllowRegularMultiply (0.0172980s)
√ AllowRegularSubtraction (0.0070800s)
√ RevertDivideBy0 (0.0499220s)

Contract: WiseMeadow.WiseTests

√ erc20_Basic_Standards (0.1053790s)
√ allowance_CheckAmountApproved_AssertAreEqual (0.0601800s)
√ transfer_ToAddressZero_ExpectRevert (0.0043360s)
√ transferFrom_ToAccountZero_Revert (0.0357930s)
√ transferFrom_ApproveThenTransfer_EmitEvent (0.0410290s)
√ canMint_MintingFinishedTrue_ExpectRevert (0.0199700s)
√ hasMintPermission_NotOwner_ExpectRevert (0.0100710s)
√ decreaseApproval_DecreaseByHalf_EmitEvent (0.0383560s)

Contract: WiseMeadow.WiseTests
√ finishMinting_CallByOwner_EmitEvent (0.0193090s)
√ decreaseApproval_Success (0.0367810s)
√ balanceOf_CheckOwnerBalance_AssertEqual (0.0030080s)
√ totalSupply_CheckTotalSupply_AssertTotal (0.0027990s)
√ increaseApproval_Success (0.0152720s)

Contract: WiseMeadow.WiseTests
√ decreaseApproval_DecreaseMoreThanAllowed_SetAllowedZero (0.0468810s)
√ transferFrom_valueGreatThanAllowed_Revert (0.0400350s)
√ transferFrom_valueGreaterThanBalance_Revert (0.0210600s)
√ transfer_SendMoreThanBalance_ExpectRevert (0.0068370s)
√ release_AmountIsZero_ExpectRevert (0.0233480s)

Contract: WiseMeadow.WiseTokenCrowdsaleExtra
√ close_WasActive_NowClosed (0.0439230s)
√ deposit_ShouldWork (0.0288890s)
√ release_NotReleased_ExpectRevert (0.0285250s)
√ refund_StateNotActive_ExpectRevert (0.0313340s)
√ claimRefund_NotFinalized_ExpectRevert (0.0102200s)
√ CappedCrowdsaleConstructor_CapIsZero_ExpectRevert (0.0291280s)
√ RefundableCrowdsaleConstructor_CapIsZero_ExpectRevert (0.0270890s)
√ WiseTokenCrowdsaleConstructor_GoalGreaterThanCap_ExpectRevert (0.0387530s)
√ TimedCrowdsaleConstructor_OpenTimeLessThanNow_ExpectRevert (0.0219810s)

Contract: WiseMeadow.WiseTokenCrowdsaleExtra
√ RefundVaultConstructor_WalletAddressZero_ExpectRevert (0.0200110s)
√ WiseTokenCrowdsaleConstructor_TokenIsAddressZero_ExpectRevert (0.0112970s)
√ onlyWhileOpen_SaleNotBegun_ExpectRevert (0.0154830s)
√ WiseTokenCrowdsaleConstructor_RateIsZero_ExpectRevert (0.0262160s)
√ enableRefunds_StateNotActive_ExpectRevert (0.0381350s)
√ TokenTimelockConstructor_ReleaseBeforeNow_ExpectRevert (0.2229770s)
√ TimedCrowdsaleConstructor_CloseTimeLessThanNow_ExpectRevert (0.0233790s)
√ deposit_MustBeActive_ExpectRevert (0.0379640s)

Appendix A

Contract: WiseMeadow.WiseTokenCrowdsaleExtra
- √ WiseTokenCrowdsaleConstructor_WalletIsAddressZero_ExpectRevert (0.0359410s)
- √ release_IsReleased_SafeTransfer (0.0473860s)
- √ setCrowdsaleStage_0_PrivateICO (0.0127640s)
- √ fallbackFunction_BuyTokens_VerifyBalance (0.0331960s)
- √ indexed (0.0004350s)

Contract: WiseMeadow.WiseTokenCrowdsaleTests
- √ claimRefund_GoalReachedAndAlreadyFinalized_ExpectRevert (0.2739860s)
- √ transferFrom_valueGreaterThanBalance_ExpectRevert (0.0109320s)
- √ capReached__ (0.0423470s)
- √ finalize_GoalReached_ (0.2382660s)
- √ transfer_ToAddressZero_ExpectRevert (0.0115460s)

Contract: WiseMeadow.WiseTokenCrowdsaleTests
- √ buyTokens_PrivateICOStage_EmitEvent (0.1163600s)
- √ buyTokens_ICOStage_EmitEvent (0.0681040s)
- √ buyTokens_BeneficiaryIsAddressZero_ExpectRevert (0.0118550s)
- √ claimRefund_PreICOStageRefund_EmitEvent (0.0728180s)
- √ getUserContribution (0.0599220s)
- √ finalize_SaleNotClosed_ExpectRevert (0.0081930s)
- √ wallet_WalletAddress_ReturnWallet (0.0642400s)
- √ preValidatePurchase_ContributionLessThanCap_ExpectRevert (0.0185200s)
- √ token_TokenERC20_ReturnToken (0.0766280s)

Contract: WiseMeadow.WiseTokenCrowdsaleTests
- √ buyTokens_PrivateICOStage_3TimesTokens (0.0910110s)
- √ buyTokens_PreICOStage_3TimesTokens (0.0916520s)
- √ rate_RateAmount_AssertRate (0.0784430s)
- √ preValidatePurchase_WeiGreaterThanCap_ExpectRevert (0.0289870s)
- √ indexed (0.1247800s)
- √ owner_SenderIsOwner_AssertOwner (0.0766360s)
- √ setCrowdsaleStage_2_ICO (0.0046770s)
- √ transfer_SendMoreThanBalance_ExpectRevert (0.0063830s)

Contract: WiseMeadow.WiseTokenCrowdsaleTests
√ finalize_SenderIsNotFounder_ExpectRevert (0.0198280s)
√ setCrowdsaleStage_SetNoStage_ (0.0229740s)
√ setCrowdsaleStage_1_PreICO (0.0111810s)
√ indexed (0.0007920s)
√ buyTokens_WeiAmountIsZero_ExpectRevert (0.0108150s)

Contract: WiseMeadow.WiseTokenCrowdsaleTests
√ closingTime_CheckClosing_AssertTime (0.0783420s)
√ openingTime_CheckOpening_AssertTime (0.0786190s)

Appendix B

FILE	FINGERPRINT
WiseCrowdsale.sol	7236676CCED2C328157F5747AB862E8C24B1F631C4B5634B49DBC8BB43049D1D
WiseToken.sol	C866B3B7C47380E7982D2C3B35D3E8335B90926142FFB9C858C9FC1F12D13FAD
Crowdsale.sol	1A745C33558C3605C507A0B505BE36113B6682385E6EA9555F08B8E604F89D09
FinalizableCrowdsale.sol	E50BA9945040E1CDE6CF770F546C130ABE553028F3051A55D786848130E18BCA
RefundableCrowdsale.sol	B88B88432F1381E829C2067396CBF61AAC3E277AED91110C46E7F5E00A912D88
RefundVault.sol	7A0B97D721069F85A3EAF8F0CC537FF9ACF6272E03EA0C04D1068D7C7138B9DB
MintedCrowdsale.sol	0E57B33F837FB5EF4A77F3A4CA6E96AA300B8FF2A52DF2EBD260E6792A2995CE
CappedCrowdsale.sol	8FFB12A4ABC0C2290796F3FE817F34D06D5ACFFC69E9B163FBF720855FBE967C
TimedCrowdsale.sol	C560145F36F670E8671C0A574DFAD2CB1AA5AF8D7CA12DBA18F9E4F3C66B3934
Pausable.sol	1651888C7D9D07418C3DA274E3598DCA7686875263EE61AD200F3E3DB67B518A
SafeMath.sol	6966B7304174D895637 70AB3B56E06AA3E20EA066B14CA84A57E13EC10A749FE
Ownable.sol	A4BD745530FEB0C27175755137 0D047235E26FE79DA2FA260F3B81715CD0A147
BasicToken.sol	2CE519DCADB6455185E1478DDEB47520A7A00F6F311F69969F6AC00315F66206
DetailedERC20.sol	98B4E1E87CFB212953D0A66F1C9E64F7E3D97A7723072D66628F7A9AC5E44B26
ERC20.sol	ED00FE45C0DEEF6A6F741C1DC57C4B5D4754404E02A3EA36DA2FAD8157CF4E1F
ERC20Basic.sol	7D99160795719766F3DC95D53B24C87AC6A0235429992AD63ECCD48BE34241CB
MintableToken.sol	2D350A87BE1F29E7560B62F4D83C329E57D2B5D22C4C80CD01DFC97FA4D61637
PausableToken.sol	83A3059F9126E6F3BA7CCD5567B6337142011BA3863CF49C45103755E3B5658E
SafeERC20.sol	F475424814B282B1C2F5799BFA6D66A30527D55C7090EF6A11CBEB421F6EF06C
StandardToken.sol	66D9D19928143A013B093E56ADDD3641485B662B108AE10EA8F51BCC9912CA0C
TokenTimelock.sol	302A09EB6AF84FD977B0440C36DEFF18261898E4EF0CCF4A32C00E166D0AFA4D

Appendix C

FILE	% BRANCHES	% FUNCTION	% LINES
WiseCrowdsale.sol	91.67%	100%	100%
WiseToken.sol	100%	100%	100%
Crowdsale.sol	100%	75%	92.31%
FinalizableCrowdsale.sol	100%	100%	100%
RefundableCrowdsale.sol	100%	100%	100%
RefundVault.sol	100%	100%	100%
MintedCrowdsale.sol	50%	100%	100%
CappedCrowdsale.sol	100%	100%	100%
TimedCrowdsale.sol	100%	100%	100%
Pausable.sol	100%	100%	100%
SafeMath.sol	100%	100%	100%
Ownable.sol	100%	100%	100%
BasicToken.sol	100%	100%	100%
DetailedERC20.sol	100%	100%	100%
ERC20.sol	100%	100%	100%
ERC20Basic.sol	100%	100%	100%
MintableToken.sol	100%	100%	100%
PausableToken.sol	100%	100%	100%
SafeERC20.sol	16.67%	33.33%	33.33%
StandardToken.sol	100%	100%	100%
TokenTimelock.sol	100%	100%	100%
ALL FILES	92.86%* (104/112)	93.75%* (60/64)	98.18%* (216/220)

* Totals are calculated using weighted percentages