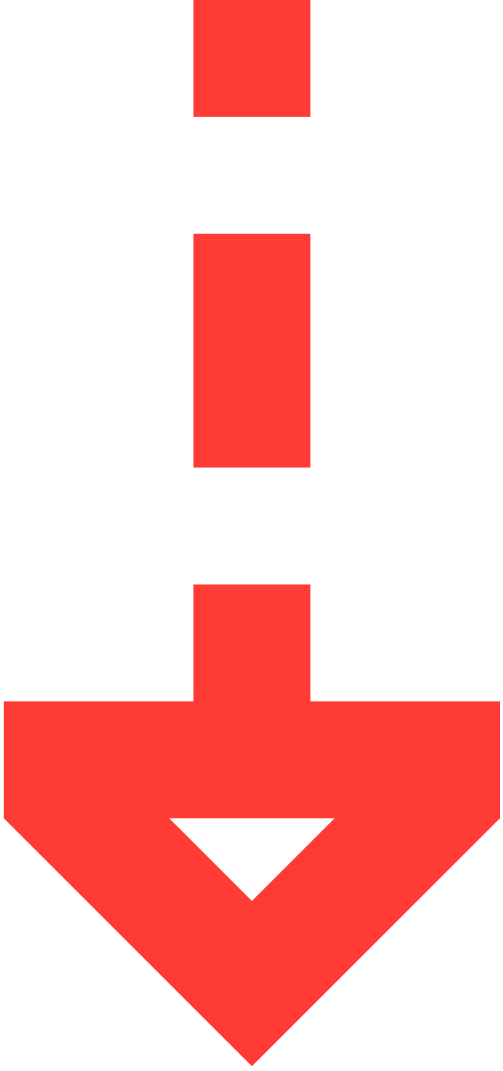
Einstein Capital Partners

Contract Audit



REPORT DATE	**June 17th, 2019**
REPORT VERSION	**1.0**

PREPARED BY

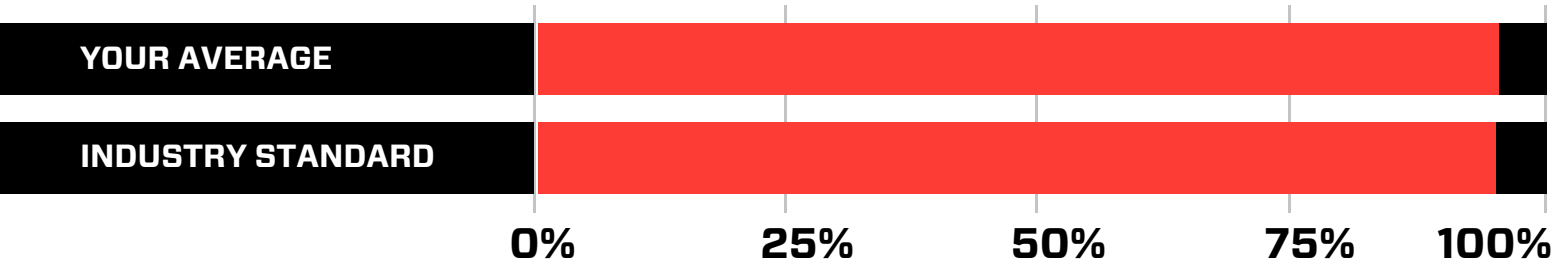
HOSHO

This document outlines the overall security of Einstein Capital Partners's smart contract as evaluated by Hosho's Smart Contract auditing team. The scope of this audit was to analyze and document Einstein Capital Partners'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 95.37%, 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 Einstein Capital Partners 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 June 3rd, 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 Einstein Capital Partners'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 EinsteinCash contract is an ERC-20 token that properly implement the ERC-20 standards, makes use of a pausable token system, and utilizes burnable functionality to dispose of tokens when needed.

2.2 Coverage Report

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

- Branches: 86.11%
- Functions: 100%
- Lines: 100%

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.

No issues found!

We are grateful to have been given the opportunity to work with the Einstein Capital Partners team.

The team of experts at Hosho, having backgrounds in all aspects of blockchain, cryptography, and cybersecurity, can say with confidence that the EinsteinCash contracts are free of any critical issues, having passed the rigorous Hosho 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 Einstein Capital Partners team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

Test Suite Results

Contract: Einstein.EinsteinTests

√ erc20_Basic_Standards (0.3344050s)
√ addPauser_AlreadyHasRole_ExpectRevert (0.0423320s)
√ decreaseApproval_DecreaseMoreThanAllowed_SetAllowedZero (0.0823830s)
√ allowance_CheckAmountApproved_AssertAreEqual (0.1601750s)
√ decreaseApproval_Success (0.0477140s)
√ renouncePauser_AddThenRemove_NoRole (0.0612040s)
√ transferFrom_valueGreatThanAllowed_Revert (0.0563110s)
√ transferFrom_valueGreaterThanBalance_Revert (0.0351970s)
√ approve_ApproveAddressZero_ExpectRevert (0.0105990s)
√ decreaseApproval_SpenderisAddressZero_ExpectRevert (0.0308290s)
√ transferFrom_ApproveThenTransfer_EmitEvent (0.0344370s)
√ balanceOf_CheckOwnerBalance_AssertEqual (0.1249880s)
√ addPauser_AddToRole_Added (0.0835570s)
√ increaseApproval_SpenderisAddressZero_ExpectRevert (0.0206410s)
√ increaseApproval_Success (0.0316910s)
√ unpause_NotPaused_ExpectRevert (0.0808540s)
√ pause_IsPaused_AssertFalse (0.0873220s)
√ transfer_SendMoreThanBalance_ExpectRevert (0.0097340s)
√ totalSupply_CheckTotalSupply_AssertTotal (0.0039480s)
√ pause_Pause_EmitEvent (0.0989810s)
√ burn_burnTokens_Assert (0.0808290s)
√ transferFrom_ToAccountZero_Revert (0.0593170s)
√ paused_IsPaused_AssertFalse (0.1141660s)
√ unpause_Pause_EmitEvent (0.0989950s)
√ decreaseApproval_DecreaseByHalf_EmitEvent (0.1739210s)
√ renouncePauser_NoRole_ExpectRevert (0.0487430s)
√ addPauser_NotPauser_ExpectRevert (0.0409640s)
√ transfer_ToAddressZero_ExpectRevert (0.0060980s)
√ burnFrom_FromAccount_EmitBurnEvent (0.1008040s)

Contract: Einstein.SafeMathTests

√ mod_dividendisNotZero_shouldReturnCorrectValue (0.0223180s)

Appendix A

Contract: Einstein.SafeMathTests

- √ mod_dividendIsZero_shouldRevert (0.0296920s)
- √ RevertAdditionOverflow (0.0347440s)
- √ RevertSubtractionOverflow (0.0258470s)
- √ RevertDivideBy0 (0.0433160s)
- √ AllowRegularDivision (0.0546530s)
- √ AllowRegularMultiply (0.0475750s)
- √ AllowRegularAddition (0.0444050s)
- √ AllowRegularSubtraction (0.0397970s)
- √ RevertMultiplyOverflow (0.0766040s)
- √ SkipOperationMult0 (0.0143260s)

Appendix B

FILE	FINGERPRINT
EinsteinCash-Flattened.sol	2B17D54F12C27AE5810CA60FCCD8347F05709B378C7FA40590EC81F1D6BCCC65

Appendix C

FILE	% BRANCHES	% FUNCTION	% LINES
EinsteinCash-Flattened.sol	86.11%	100%	100%
ALL FILES	86.11%* (31/36)	100%* (43/43)	100%* (89/89)

* Totals are calculated using weighted percentages