HackSafe

Smart Contract Security Audit Report

FaithCoin

September 2022

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
FaithCoin

Deployer address
0x2cE3a2c1670562759dA59831FADbf60880bAa8e9

Client contacts
FaithCoin Team

Blockchain
Ethereum

Website
Not provided

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by FaithCoin to perform an audit of smart contract:

- https://etherscan.io/address/0xe531642e9bb5d027e9c20e03284287b97919a9a5#code

The purpose of the audit was to achieve the

- Ensutre that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 19.09.2022

Token Type	: ERC20
Contract name	: FaithCoin
Contract address	: 0xE531642e9bb5d027E9C20E03284287B97919a9a5
Compiler version	: v0.4.19+commit.c4cbbb05
Total supply	: 25,000,000
Token ticker	: FAITH
Decimals	: 8
Token holders	: 4,576
Transactions count	: 12,260
Contract deployer address	: 0x2cE3a2c1670562759dA59831FADbf60880bAa8e9
Owner address	: 0x2cE3a2c1670562759dA59831FADbf60880bAa8e9

Social profiles

Twitter Profile	: https://twitter.com/MyFaithCoin
Telegram profile	: https://t.me/FaithCoin
Coingecko profile	: https://www.coingecko.com/en/coins/faithcoin/

Claimed Smart Contract Features

Claimed Feature Detail

Tokenomics :

- **Name** : FaithCoin
- **Symbol** : FAITH
- **Decimals** : 8
- **Protocol** : ERC20
- **Total supply** : 25,000,000
- **Contract address** : 0xE531642e9bb5d027E9C20E03284287B97919a9a5

Our Observation

YES, this is valid.

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “secure”. This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.

Insecure	Poor secured	Secure	Well-secured

You are here 

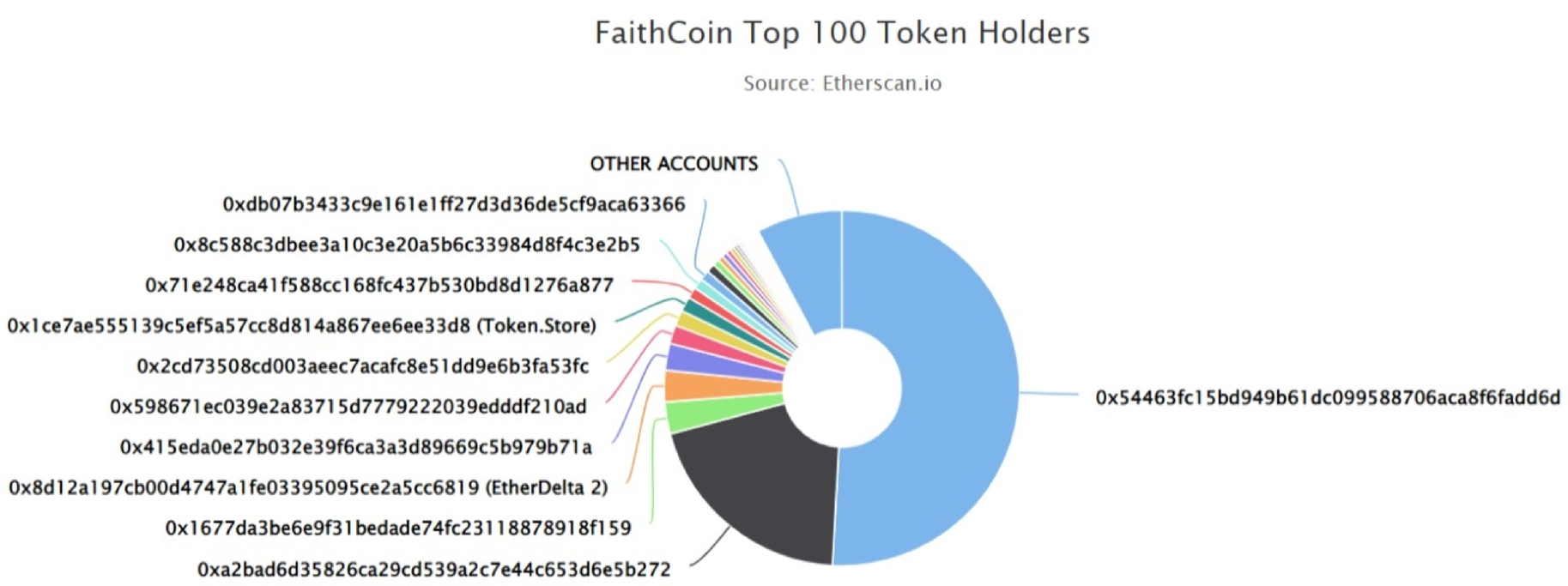
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 1 medium and 2 low and some very low-level issues.

FaithCoin Token Distribution

The top 100 holders collectively own 92.19% (23,048,684.07 Tokens) of FaithCoin

Token Total Supply: 25,000,000.00 Token | Total Token Holders: 4,576



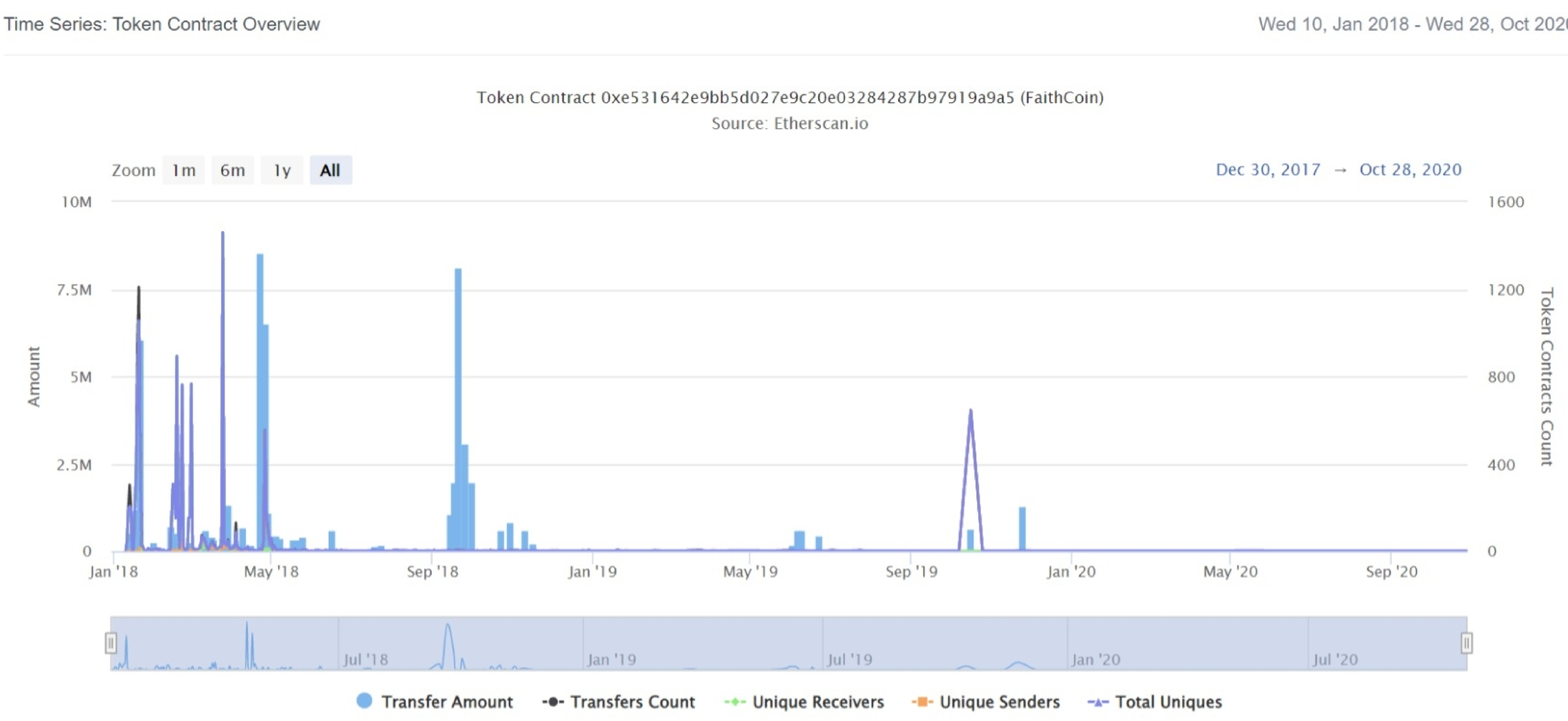
FaithCoin Top 20 Token Holders

(A total of 23,048,684.07 tokens held by the top 100 accounts from the total supply of 25,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x54463fc15bd949b61dc099588706aca8f6fadd6d	12,713,746.28383403	50.8550%
2	0xa2bad6d35826ca29cd539a2c7e44c653d6e5b272	5,000,000	20.0000%
3	0x1677da3be6e9f31bedade74fc23118878918f159	720,999	2.8840%
4	EtherDelta 2	718,255.00042072	2.8730%
5	0x415eda0e27b032e39f6ca3a3d89669c5b979b71a	607,500	2.4300%
6	0x598671ec039e2a83715d7779222039edddf210ad	423,682.8608	1.6947%
7	0x2cd73508cd003aeec7acafc8e51dd9e6b3fa53fc	352,146.2515	1.4086%
8	Token.Store	339,230.52	1.3569%
9	0x71e248ca41f588cc168fc437b530bd8d1276a877	250,000	1.0000%
10	0x8c588c3dbee3a10c3e20a5b6c33984d8f4c3e2b5	245,500	0.9820%
11	0xdb07b3433c9e161e1ff27d3d36de5cf9aca63366	225,000	0.9000%
12	0xc13dede8a7ba3bb99a65bc62945aac14bc3cd490	200,000	0.8000%
13	0x8321a402104513c4ee59c5d0245af6b3161d726e	150,000	0.6000%
14	0x161a4fc0d0281a5fd21661d711d16ee5c7de2927	125,000	0.5000%
15	0x2ce3a2c1670562759da59831fadbf60880baa8e9	116,712	0.4668%
16	0x48b2225d580508e6c9114c043090e2f67e985450	104,040.72095997	0.4162%
17	DDEX: Old Address	100,000.28933516	0.4000%
18	0xb1433a56c5c0a96f6a8953a6d1bb599169569132	70,000	0.2800%
19	0x4a48db3f42af3acc86cdc79f57e8f7bd87d132d9	61,750	0.2470%
20	0x8ec64cbc706313e67c617fb174eaaa4aa077defe	50,000	0.2000%

FaithCoin Token Distribution

FaithCoin Contract Overview



Contract functions details

+ ForeignToken
    -[Pub] balanceOf
    -[Pub] transfer

+ERC20Basic
    -[Pub] balanceOf
    -[Pub] transfer

+ERC20 (ERC20Basic)
    -[Pub] allowance
    -[Pub] transferFrom
    -[Pub] approve

+[Lib] SaferMath
    -[Int] mulX
    -[Int] divX
    -[Int] sub
    -[Int] add

+FaithCoin (ERC20)
    -[Pub] name
    -[Pub] symbol
    -[Pub] decimals
    -[Pub] FaithCoin
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Pub] getEthBalance
    -[Pub] distributeFAITH #
      -modifiers: onlyOwner canDistr
    -[Pub] balanceOf
    -[Pub] transfer #
      -modifiers: onlyPayloadSize
    -[Pub] transferFrom #
      -modifiers: onlyPayloadSize
    -[Pub] approve #
    -[Pub] allowance
    -[Pub] finishDistribution #
    -[Pub] withdrawForeignTokens #

Contract functions details

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Medium issue
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues

No critical severity issue found.

High Severity Issues

No high severity issues found.

Medium Severity Issues

One medium severity issues found.

1. Out of gas limit.

- **Description**

  The contract have used block.timestamp many times in some modifiers such as notLockedWallet as the miners here can manipulate the smart contract in order to attack the contract.

- **Recommendation**

  It is advisable to either remove for loop or use smaller length of array to avoid the gas limit error.

Low Severity Issues

Two low severity issue found.

1. Too old compiler version.

- **Description**

  Contract has been deployed using too old compiler version.

- **Recommendation**

  It is advisable that the compiler version of solidity should be among the new compiler versions.

2. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.4.16 the contract should contain the following line:

  pragma solidity 0.4.19;

Centralization

Owner Privileges :

- FaithCoin Contract:
    - Owner can distribute faith token.
    - Owner can transfer ownership.
    - Owner can finish distribution of tokens.

This smart contract has some functions which can be executed by the owner (Admin) only. If the admin wallet private key would be compromised, it would create trouble as smart contract ownership has not been renounced. Following are the only admin functions:

- Distributefaith
- Transferownership
- Finishdistribution

Conclusion

Smart contract contains low and medium severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.