



Smart Contract Security Audit Report

Amon

October 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Amon



Deployer address

0x555fCEe5760152FaE11B70a49975b4E58091D893



Client contacts

Amon Team



Blockchain

Ethereum



Website

<https://amon.tech/>

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 Amon to perform an audit of smart contracts:

- <https://etherscan.io/token/0x737f98ac8ca59f2c68ad658e3c3d8c8963e40a4c#code>

The purpose of the audit was to achieve the following:

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

The information in this report should be understood to 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 04.10.2022

Token Type	: ERC20
Contract name	: AMNToken
Contract address	: 0x737F98AC8cA59f2C68aD658E3C3d8C8963E40a4c
Total supply	: 1,666,666,667
Token ticker	: AMN
Decimals	: 18
Token holders	: 3,396
Transactions count	: 80,723
Compiler version	: v0.4.19+commit.c4cbbb05
Contract deployer address	: 0x555fCEe5760152FaE11B70a49975b4E58091D893
Owner address	: No owner

Social profiles

Twitter Profile	: https://twitter.com/amonwallet
Telegram profile	: https://t.me/amontech
Coinmarketcap profile	: https://coinmarketcap.com/currencies/amon/
Coingecko profile	: https://www.coingecko.com/en/coins/amon/

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Well Secure”**. This token contract does not contain owner control, which do make it fully decentralized as owner does not 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, 0 medium and 2 low and some very low-level issues. These issues are not critical ones.

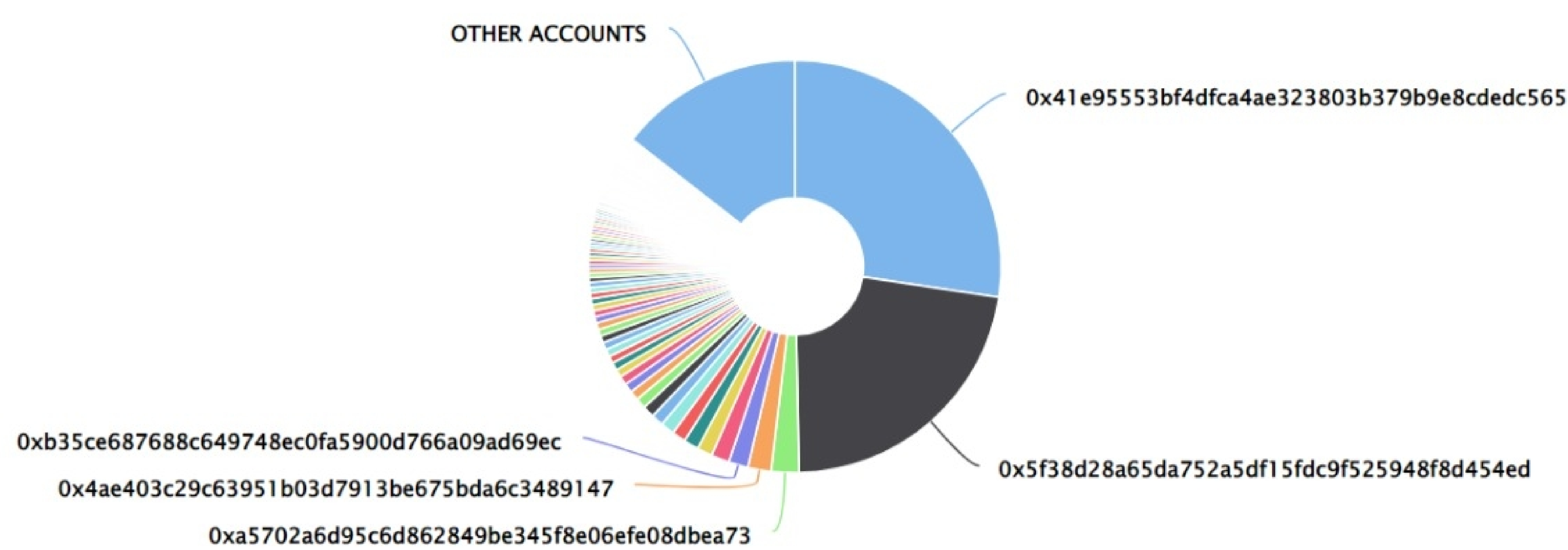
Amon Token Distribution

The top 100 holders collectively own 85.55% (1,425,889,696.49 Tokens) of Amon

Token Total Supply: 1,666,666,667.00 Token | Total Token Holders: 3,396





Amon Top 100 Token Holders

Source: Etherscan.io



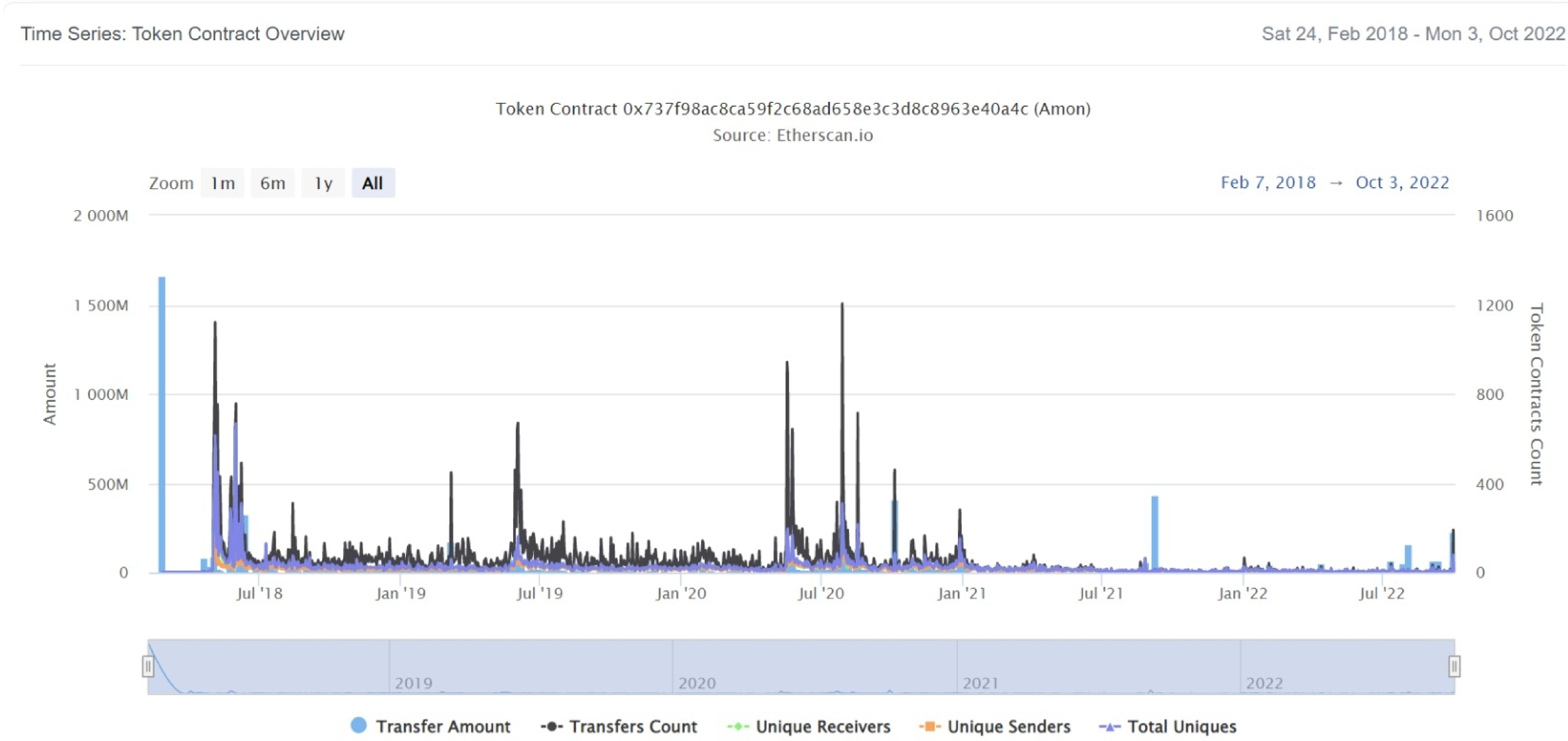
Amon Top 20 Token Holders

(A total of 1,425,889,696.49 tokens held by the top 100 accounts from the total supply of 1,666,666,667.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 0x41e95553bf4dfca4ae323803b379b9e8cdedc565	456,702,981.64	27.4022%
2	 0x5f38d28a65da752a5df15fdc9f525948f8d454ed	371,424,213.939082689447560625	22.2855%
3	 0xa5702a6d95c6d862849be345f8e06efe08dbea73	36,000,000	2.1600%
4	0x4ae403c29c63951b03d7913be675bda6c3489147	30,433,064.27908149298916214	1.8260%
5	 0xb35ce687688c649748ec0fa5900d766a09ad69ec	25,633,738.638162966226331069	1.5380%
6	0x4bae060390eb45697c034f26a46af04fe06e83ad	23,500,039.895246284824904493	1.4100%
7	0xd84850148290d91bc1dc8bc117a359cab5c5052e	20,279,461.864711037795101982	1.2168%
8	0x35638e16672079627f6887a08766882a0048e123	19,285,679.617501090861542004	1.1571%
9	0xef473b308ca522c90916e0b68509c1f2de1bf8a0	18,130,485.24	1.0878%
10	0x39925d63ce3fa1df3c2223e91eb484c72f1ed9c4	18,045,798.088460582530027407	1.0827%
11	0xf0614ed7c87a84dc7d02091ebc5ab623330a35bb	15,867,742.727107547514619883	0.9521%
12	0x8e01ef6a4d864698ff80b419fe9ec2e3c85e9e9e	15,322,064.95177938	0.9193%
13	0x94da250b232e4c251bbc31905333d2fbade57b4b	13,842,084.314800258900865164	0.8305%
14	0x82a3d828ece368222db8b71e1d1e1ad9e5688ce2	12,405,687.575921043688451542	0.7443%
15	0xa5f43c6710ff9243a42e64717f7c7b0beee4c29b	12,100,000.008517949842800058	0.7260%
16	0x1b3d794bbeecd9240f46dbb3b79f4f71a972e00a	11,903,360.710280343011577881	0.7142%
17	0x949901cf0eb0dca192d987b1e68ef9d76c597c87	10,000,500	0.6000%
18	0xbfe707108f20e84cddfb69fadcb9df3fd50e4082	9,955,452.40814402557373826	0.5973%
19	0xd9cf2fe3bf9a091209fc5a4b8bd335a22e19f874	9,682,659.340344417172466155	0.5810%
20	0xcf24c1a55d3ae5c1c4fc43cf5517ad111ad7f9b	9,590,705.013999157850519654	0.5754%

Amon Token Distribution

Amon Contract Overview



Contract functions details

+[Lib] SafeMath

- [Int] mul
- [Int] div
- [Int] sub
- [Int] add

+ERC20Basic

- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer

+BasicToken (ERC20Basic)

- [Pub] totalSupply
- [Pub] transfer #
- [Pub] balanceOf

+ERC20 (ERC20Basic)

- [Pub] allowance
- [Pub] transferFrom
- [Pub] approve

+StandardToken (ERC20, BasicToken)

- [Pub] transferFrom #
- [Pub] approve #
- [Pub] allowance
- [Pub] increaseApproval #
- [Pub] decreaseApproval #

+AMNToken (StandardToken)

- [Pub] AMNToken #

(\$) = 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.	Passed
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

No medium severity issue found.

✔ Low Severity Issues

Two low severity issue found.

1. 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 0.4.19 the contract should contain the following line:

```
pragma solidity 0.4.19;
```

2. Old Compiler Version

- **Description**

Contract has been deployed using too old solidity version.

- **Recommendation**

It is advisable to deploy contract using any of the latest version of solidity.

Conclusion

Smart contract contains low 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.