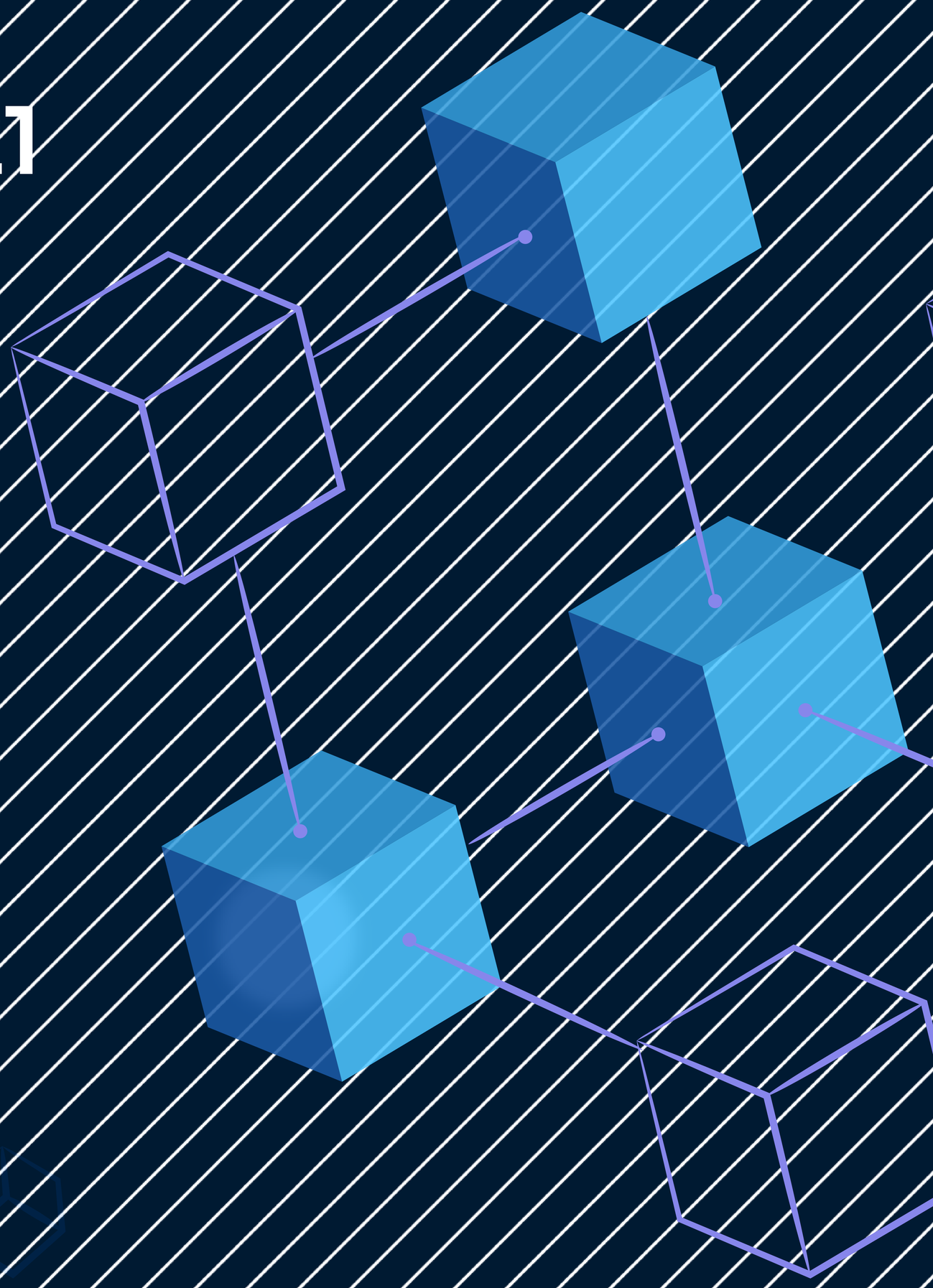
QuillAudits

Audit Report
November, 2021



For

THE AVAX LAUNCHPAD

Contents

Scope of the Audit

The scope of this audit was to analyze and document the AVX Token smart contract codebase for quality, security, and correctness.

Checked Vulnerabilities

We have scanned the smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis
In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis
Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis
Manual analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption
In this step, we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit
Remix IDE, Truffle, Truffle Team, Solhint, Mythril, Slither, Solidity statistic analysis, Theo.

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

Risk-level	Description
High	A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.
Medium	The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.
Low	Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.
Informational	These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Number of issues per severity

Type	High	Medium	Low	Informational
Open	0	0	0	0
Acknowledged	0	0	2	3
Closed	0	0	0	0

Introduction

During the period of **November 21, 2021 to November 25, 2021** - QuillAudits Team performed a security audit for **AVX** smart contracts.

The code for the audit was taken from following the official link: https://polygonscan.com/address/0xca919a0981cd207d2b6121e832166cd6fc87b14f#code

Ver No.	Date	Commit hash	Files
1	November	https://polygonscan.com/address/0xca919a0981cd207d2b6121e832166cd6fc87b14f#code	1

Issues Found

A. Contract – AVX

High severity issues

No issues were found.

Medium severity issues

No issues were found.

Low severity issues

1. **Missing zero address validation**

Line	Code

19-21	function changeOwnership(address payable _newOwner) public
	onlyOwner {
	owner = _newOwner;
	}

197-199	function setAddressToChange(address addr) public onlyOwner {
	addressToBeChanged = addr;
	}

203-205	function setAddressToSend(address addr) public onlyOwner {
	addressToSend = addr;
	}

Description

When setting the new owner address, it should be checked for **zero address**. Otherwise, they may lose the ability to use the privileged functions.

Similarly, the addressToBeChanged and addressToSend should be checked for zero address. Otherwise, tokens sent to the zero address may be burnt forever.

Remediation

Use the **require** statement to check for zero addresses.

Status: Acknowledged

2. ERC20 approve() race-condition

Description
Using approve() to manage allowances opens yourself and users of the token up to front-running. Changing an allowance with this method brings the risk that someone may use both the old and the new allowance by unfortunate transaction ordering.
Read more

Remediation
Implement the Openzeppelin's ERC20 increaseAllowance and decreaseAllowance functions.

Status: Acknowledged

Informational issues

3. Missing Events for Significant Transactions

Description
The missing event makes it difficult to track off-chain decimal changes.
An event should be emitted for significant transactions calling the functions :
- changeOwnership
- setChangeStatus
- setPercent
- setAddressToChange
- setAddressToSend

Remediation
We recommend emitting the appropriate events.

Status: Acknowledged

4. Public function that could be declared external

Description
The following public functions that are never called by the contract should be declared external to save gas:
- changeOwnership
- setChangeStatus
- setPercent
- setAddressToChange
- setAddressToSend

Remediation
Use the external attribute for functions never called from the contract.

Status: Acknowledged

5. Floating pragma

```
pragma solidity ^0.8.6;
```

Description
The contract makes use of the floating-point pragma ^0.8.6 Contracts should be deployed using the same compiler version and flags that were used during the testing process. Locking the pragma helps ensure that contracts are not unintentionally deployed using another pragma, such as an obsolete version that may introduce issues in the contract system.

Remediation
Lock the pragma

Status: Acknowledged

Functional Test Cases

- Should be able to transfer/transferFrom **PASS**
- Burn should decrease totalSupply **PASS**
- Mint by owner should increase totalSupply **PASS**
- Transfer/TransferFrom to special address should take fees **PASS**
- totalSupply should equal the specified amount **PASS**

Automated Tests

Slither

```
Owned.changeOwnership(address) (AVX.sol#19-21) should emit an event for:
        - owner = _newOwner (AVX.sol#20)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-access-control

ERC20.setAddressToChange(address).addr (AVX.sol#197) lacks a zero-check on :
                - addressToBeChanged = addr (AVX.sol#198)
ERC20.setAddressToSend(address).addr (AVX.sol#203) lacks a zero-check on :
                - addressToSend = addr (AVX.sol#204)
Owned.changeOwnership(address)._newOwner (AVX.sol#19) lacks a zero-check on :
                - owner = _newOwner (AVX.sol#20)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation

ERC20.transfer(address,uint256) (AVX.sol#49-77) compares to a boolean constant:
        -change == true (AVX.sol#53)
ERC20.transferFrom(address,address,uint256) (AVX.sol#87-119) compares to a boolean constant:
        -change == true (AVX.sol#92)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#boolean-equality

Different versions of Solidity is used:
        - Version used: ['>=0.4.22<0.9.0', '^0.8.6']
        - ^0.8.6 (AVX.sol#6)
        - >=0.4.22<0.9.0 (Migrations.sol#2)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used

Pragma version^0.8.6 (AVX.sol#6) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version>=0.4.22<0.9.0 (Migrations.sol#2) is too complex
solc-0.8.6 is not recommended for deployment
```

```
Parameter Owned.changeOwnership(address)._newOwner (AVX.sol#19) is not in mixedCase
Parameter ERC20.balanceOf(address)._owner (AVX.sol#41) is not in mixedCase
Parameter ERC20.transfer(address,uint256)._to (AVX.sol#49) is not in mixedCase
Parameter ERC20.transfer(address,uint256)._amount (AVX.sol#49) is not in mixedCase
Parameter ERC20.transferFrom(address,address,uint256)._from (AVX.sol#87) is not in mixedCase
Parameter ERC20.transferFrom(address,address,uint256)._to (AVX.sol#87) is not in mixedCase
Parameter ERC20.transferFrom(address,address,uint256)._amount (AVX.sol#87) is not in mixedCase
Parameter ERC20.approve(address,uint256)._spender (AVX.sol#126) is not in mixedCase
Parameter ERC20.approve(address,uint256)._amount (AVX.sol#126) is not in mixedCase
Parameter ERC20.allowance(address,address)._owner (AVX.sol#136) is not in mixedCase
Parameter ERC20.allowance(address,address)._spender (AVX.sol#136) is not in mixedCase
Parameter ERC20.setPercent(uint256)._percent (AVX.sol#191) is not in mixedCase
Variable Migrations.last_completed_migration (Migrations.sol#6) is not in mixedCase
 Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

 AVX.constructor() (AVX.sol#218-228) uses literals with too many digits:
         - totalSupply = 21000000 * 10 ** 18 (AVX.sol#222)
 Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

 changeOwnership(address) should be declared external:
         - Owned.changeOwnership(address) (AVX.sol#19-21)
 balanceOf(address) should be declared external:
         - ERC20.balanceOf(address) (AVX.sol#41)
 transfer(address,uint256) should be declared external:
         - ERC20.transfer(address,uint256) (AVX.sol#49-77)
transferFrom(address,address,uint256) should be declared external:
         - ERC20.transferFrom(address,address,uint256) (AVX.sol#87-119)
approve(address,uint256) should be declared external:
         - ERC20.approve(address,uint256) (AVX.sol#126-131)
allowance(address,address) should be declared external:
         - ERC20.allowance(address,address) (AVX.sol#136-138)
setChangeStatus(bool) should be declared external:
         - ERC20.setChangeStatus(bool) (AVX.sol#184-188)
setPercent(uint256) should be declared external:
         - ERC20.setPercent(uint256) (AVX.sol#191-193)
setAddressToChange(address) should be declared external:
         - ERC20.setAddressToChange(address) (AVX.sol#197-199)
setAddressToSend(address) should be declared external:
         - ERC20.setAddressToSend(address) (AVX.sol#203-205)
setCompleted(uint256) should be declared external:
         - Migrations.setCompleted(uint256) (Migrations.sol#16-18)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
. analyzed (4 contracts with 75 detectors), 35 result(s) found
```

Results

No major issues were found. Some false positive errors were reported by the tool. All the other issues have been categorized above according to their level of severity.

Closing Summary

Overall, smart contracts are very well written and adhere to guidelines.

No instances of Integer Overflow and Underflow vulnerabilities or Back-Door Entry were found in the contract, but relying on other contracts might cause Reentrancy Vulnerability.

Two Low Severity Issues found during the Audit which has been Acknowledged by the AVX Team.

Disclaimer

Quillhash audit is not a security warranty, investment advice, or an endorsement of the **AVX** platform. This audit does not provide a security or correctness guarantee of the audited smart contracts. 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. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the **AVX** Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

Audit Report
November, 2021

For

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com