Security Assessment

AANN.ai

Verified On March 13th, 2024

@Vital-Block

@VB_Audit

info@vitalblock.org

www.vitalblock.org

PREPARED FOR:

AANN.ai

TABLE OF CONTENTS

INTRODUCTION

Auditing Firm	**VITAL BLOCK SECURITY**
Client Firm	**AANN.ai**
Methodology	**Automated Analysis, Manual Code Review.**
Language	**Solidity**
Contract	**ANToken.sol** **ANTokenMultichain.sol**
Source Code Light	**Open Source**
License	**MIT**
Centralization	**Active ownership**
Compiler Version	**^0.8.19**
Network	**BSC NETWORK**
Website	**https://aann.ai/**
Telegram	**https://t.me/aann_network**
Twitter	**https://twitter.com/aann_ai**
Doc	**https://aann-ai.gitbook.io/social-authenticity-network/**
Prelim Report Date	**MARCH 12th 2024**
Final Report Date	**MARCH 13TH 2024**

Verify the authenticity of this report on our GitHub Repo: https://www.github.com/vital-block

Document Properties

Client	AANN.ai
Title	Smart Contract Audit Report
Target	AANN.ai
Audit Version	1.0
Author	Akhmetshin Marat
Auditors	Akhmetshin Marat, James BK, Benny Matin
Reviewed by	Dima Meru
Approved by	Prince Mitchell
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	March 13th, 2024	James BK	Final Released
1.0-AP	March 13th , 2024	Benny Matin	Release Candidate

Contact

For more information about this document and its contents, please contact Vital Block Security Inc.

Name	Akhmetshin Marat
Phone	+44 7944 248057
Email	info@vitalblock.org

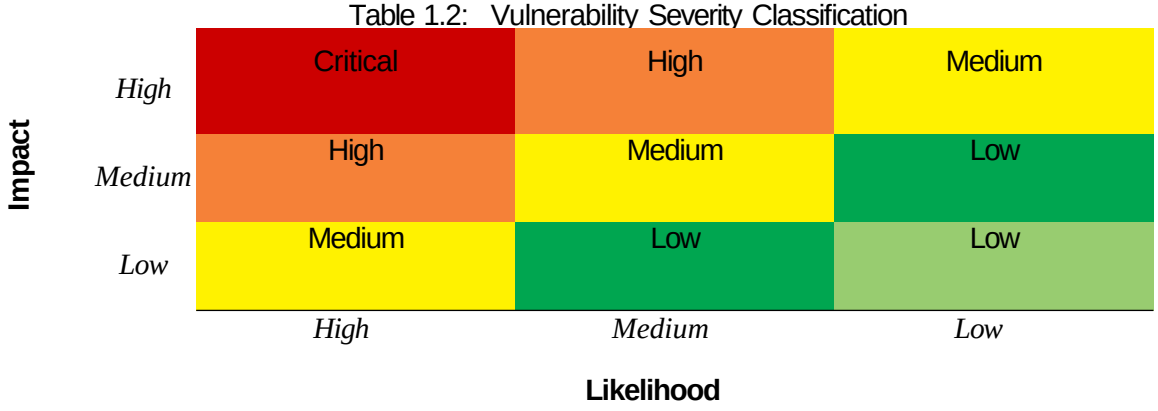
In the following, we show the specific pull request and the commit hash value used in this audit.

- https://github.com/aann-ai (AANR87221)
- https://github.com/aann-ai/contracts/tree/main/contracts (AAN7752)

About Vital Block Security

Vital Block Security provides professional, thorough, fast, and easy-to-understand smart contract security audit. We do in-depth and penetrative static, manual, automated, and intelligent analysis of the smart contract. Some of our automated scans include tools like ConsenSys MythX, Mythril, Slither, Surya. We can audit custom smart contracts, DApps, Rust, NFTs, etc (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/vital_block), Twitter (http://twitter.com/Vb_Audit), or Email (info@vitalblock.org).

Table 1.2: Vulnerability Severity Classification



Methodology (1)

To standardize the evaluation, we define the following terminology based on the OWASP Risk Rating Methodology [4]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

SCOPE OF WORK

Vital Block was consulted by AANN to conduct the smart contract audit of its Sol source code. The audit scope of work is strictly limited to mentioned .SOL file only.

```
O.ANToken.sol
O.ANTokenMultichain.sol
```

External contracts and/or interfaces dependencies are not checked due to being out of scope.

Verify audited contract code Repo.

Public Contract Code Link:
https://github.com/aann-ai/contracts/blob/main/contracts/ANToken.sol https://github.com/aann-ai/contracts/blob/main/contracts/ANTokenMultichain.sol

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of Vital Block Security auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
  - Remix IDE Developer Tool
  - Open Zeppelin Code Analyzer
  - SWC Vulnerabilities Registry
  - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges. We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	○ Token Supply Manipulation ○ Access Control and Authorization ○ Assets Manipulation ○ Ownership Control ○ Liquidity Access ○ Stop and Pause Trading ○ Ownable Library Verification

Common Contract Vulnerabilities	○ Integer Overflow ○ Lack of Arbitrary limits ○ Incorrect Inheritance Order ○ Typographical Errors ○ Requirement Violation ○ Gas Optimization ○ Coding Style Violations ○ Re-entrancy ○ Third-Party Dependencies ○ Potential Sandwich Attacks ○ Irrelevant Codes ○ Divide before multiply ○ Conformance to Solidity Naming Guides ○ Compiler Specific Warnings ○ Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to the codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH

- The client may use the audit report internally or disclose it publicly.

It is important to note that there is no pass or fail in the audit, it is recommended to view the audit as an unbiased assessment of the safety of solidity codes.

Table 1.0 The Full Audit Checklist

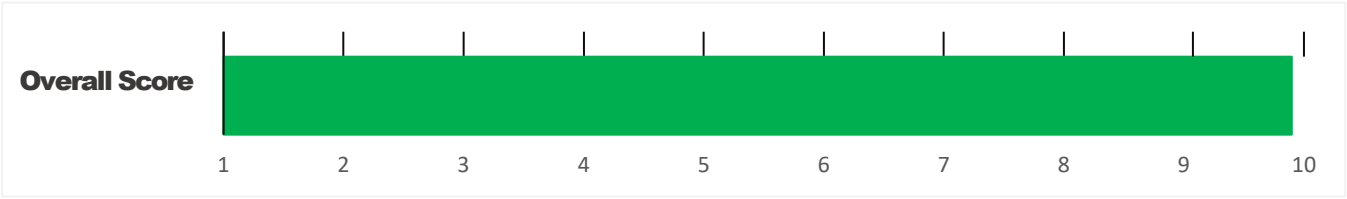
Category	Checklist Items
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

EXECUTIVE SUMMARY

Vital Block Security has performed the automated and manual analysis of the AANN Sol code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical ! 🔴	Major " 🟠	Medium # 🟡	Minor $ 🟢	Unknown 🟤
Open	0	0	0	0	2
Acknowledged	0	0	0	2	1
Resolved	0	0	1	0	2
Noteworthy OnlyOwner Privileges	Set Taxes and Ratios, Airdrop, Set Protection Settings, Set Reward Properties, Set Reflector Settings, Set Swap Settings, Set Pair and Router				

AANN.ai Smart contract has achieved the following score: 98.5



ℹ **Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.**

ℹ **Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.**

CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- **Privileged roles can be granted the power to** pause() **the contract in case of an external attack.**
- **Privileged roles can use functions like,** include(), **and** exclude() **to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.**

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- **The client can lower centralization-related risks by implementing below mentioned practices:**
- **Privileged role's private key must be carefully secured to avoid any potential hack.**
- **Privileged role should be shared by multi-signature (multi-sig) wallets.**
- **Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.**
- **Renouncing the contract ownership, and privileged roles.**
- **Remove functions with elevated centralization risk.**

ℹ️ **Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.**

RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical ! 🔴	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major " 🟠	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium # 🟡	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor $ 🟢	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown % 🟤	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.

AUDIT SCOPE | Ai Social Authenticity Network

ID	Repo	Comment	File	SHM321 Checksum
LBY	contracts/ANToken	cC512486	**ANToken.sol**	6788099YIRHVSK853PKFMGHEF44309200KDHFCBUGIJN
LBI	contracts/ANToken	cC512486	**ANToken.sol**	347520JHDB7549H22H3BVDIOETYUHF009JBIKBDI33BJ4
LBW	contracts/ANToken	cC512486	**ANToken.sol**	1988Y73HUGFDINN353840NFMTEJER73649RGFIMDIDH
LBG	contracts/ANTokenMultichain	cC512486	**ANTokenMultichain.sol**	4438648TEOHBF6378309EHROECNEPOEJDNETE8EYEU3
LBL	contracts/ANTokenMultichain	cC512486	**ANTokenMultichain.sol**	66390028765RVNKDBYFTGW553T2KOEHIUUJJIJE
LBA	contracts/ANTokenMultichain	cC512486	**ANTokenMultichain.sol**	09825539BDYG543DVNKOMIKEBYRJUFHHFHJFIE333222
LBJ	contracts/interfaces	cC512486	**IANToken.sol**	8654RJVT3DWI865YK26437903JJDGGDHGWY6E
LBE	contracts/interfaces	cC512486	**IANToken.sol**	7763888636TGYGFFTFHBETT66TFTCTVYBHBYT
LBP	contracts/interfaces	cC512486	**IANToken.sol**	88530486494YRHFTEICBGEIEGWTWYWUHEJEHEIE33U3
LBM	contracts/interfaces	cC512486	**IANTokenMultichain.sol**	1209873KHJLKJNFJHGE98763990029774BCUHHDUU239
LBV	contracts/interfaces	cC512486	**IANTokenMultichain.sol**	23456UGFYUHE98756EFHJHE7654ESDFGHGERTYUJ3897
LBQ	contracts/interfaces	cC512486	**IANTokenMultichain.sol**	37889UHBIONEO7TYRDFGVBN5678939IJWSFVDYUHDCI
LBS	contracts/interfaces	cC512486	**IWormholeReceiver.sol**	678903098TFHJKFCPOIUGFGHJKE9865ERGBEIVBHE8767
LBR	contracts/interfaces	cC512480	**IWormholeReceiver.sol**	98765SDFGBNFCOI56789UIYHGGHEJDIUYTRDCVBN3459
LCD	contracts/interfaces	cC512481	**IWormholeReceiver.sol**	3348y9808hgtrusvnmu43100ejfojgfnut8496230hb574he
LHU	contracts/interfaces	cC512481	**IWormholeRelayer.sol**	9864byf5f379eig28ffre64085jv1613251guhkdmue87
LGG	contracts/interfaces	cC512481	**IWormholeRelayer.sol**	7ej2d8jg765tjfiowg538ij74dwftyv6478ij3gs820
LTR	contracts/interfaces	cC512481	**IWormholeRelayer.sol**	864fr46de438hdguw903rfdcb246dbuhb2917enk

Key Findings

Overall, these contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), 0 medium-severity vulnerabilities, 3 low-severity vulnerabilities, and 1 informational recommen- dations.

Table 2.1: Key **AANN** Audit Findings

ID	Severity	Title	Category	Status
AN-01	Low	In updateForOwner, Relevant Function Snippet	Coding Practice	Fixed
AN-002	Informational	In Unchecked Transfer , the following equation is used inside an unchecked block	Business Logic	Fixed
AN-03	Low	In updateForMinter , the following equation is used inside an unchecked block	Status Mathematical Operations	Acknowledged
AN-04	Low	In updateForAmount, Relevant Function Snippet	Multiple Contracts	Acknowledged

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to page 10 for details.

AUTOMATED ANALYSIS

Symbol	Definition
🛑	**Function modifies state**
💵	**Function is payable**
🔒	**Function is internal**
🔐	**Function is private**
❗	**Function is important**

** **ANToken** **	Interface			
└	totalSupply	External ❗		❗		NO❗
└	decimals	External ❗		❗		NO❗
└	symbol	External ❗		❗		NO❗
└	name	External ❗		❗		NO❗
└	getOwner	External ❗				NO❗
└	balanceOf	External ❗		❗		NO❗
└	transfer	External ❗	"	❗	🛑	|NO❗
└	allowance	External ❗		❗		NO❗
└	approve	External ❗	"	❗	🛑	|NO❗
└	transferFrom	External ❗	"			NO❗

IFactoryV2	Interface		
└	getPair	External ❗		|NO❗
└	createPair	External ❗	"	|NO❗

IV2Pair	Interface		
└	factory	External ❗		|NO❗
└	getReserves	External ❗		|NO❗
└	sync	External ❗	"	|NO❗

IRouter01	Interface			
└	factory	External ❗		|NO❗
└	ETH	External ❗		|NO❗
└	addLiquidityETH	External ❗		# |NO❗
└	addLiquidity	External ❗	"	|NO❗
└	swapExacETHForTokens	External ❗		# |NO❗
└	getAmountsOut	External ❗		|NO❗
└	getAmountsIn	External ❗		|NO❗
IRouter02	Interface	IRouter01		
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	"	|NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗		# |NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	" ! 🛑 |NO❗
└	swapExactTokensForTokens	External ❗	"	|NO❗
Protections	Interface			
└	checkUser	External ❗	" ! 🛑 |NO❗
└	setLaunch	External ❗	" ! 🛑 |NO❗
└	setLpPair	External ❗	" ! 🛑 |NO❗
└	AN	External ❗	" |NO❗
└	removeSniper	External ❗	" |NO❗
Cashier	Interface			
└	setRewardsProperties	External ❗	"	|NO❗
└	tally	External ❗	" |NO❗
└	load	External ❗		# |NO❗
└	cashout	External ❗	"	|NO❗
└	giveMeWelfarePlease	External ❗	"	|NO❗
└	getTotalDistributed	External ❗		|NO❗
└	getUserInfo	External ❗		|NO❗
└	getUserRealizedRewards	External ❗		|NO❗

| └ | getPendingRewards | External ❗ | | |NO❗ |

| └ | initialize | External ❗ | " | |NO❗ |

| └ | getCurrentReward | External ❗ | | |NO❗ |

||||||

| **SOL** | Implementation | SafeMath |||

| └ | <Constructor> | Public ❗ | | # |NO❗ |

| └ | transferOwner | External ❗ | " | | onlyOwner |

| └ | renounceOwnership | External ❗ | " | | NO❗|

| └ | setOperator | Public ❗ | " | |NO❗ |

| └ | renounceOriginalDeployer | External ❗ | " | |NO❗ |

| └ | <Receive Ether> | External ❗ | | # |NO❗ |

| └ | totalSupply | External ❗ | | |NO❗ |

| └ | decimals | External ❗ | | |NO❗ |

| └ | symbol | External ❗ | | |NO❗ |

| └ | name | External ❗ | | |NO❗ |

| └ | getOwner | External ❗ | | ! |NO❗ |

| └ | balanceOf | Public ❗ | | ! |NO❗ |

| └ | allowance | External ❗ | | ! |NO❗ |

| └ | approve | External ❗ | " | ! 🛑 |NO❗ |

| └ | _approve | Internal $ | " | | |

| └ | approveContractContingency | Public ❗ | " | ! 🛑 | onlyOwner |

| └ | transfer | External ❗ | " | |NO❗ |

| └ | transferFrom | External ❗ | " | |NO❗ |

| └ | setNewRouter | External ❗ | " | | onlyOwner |

| └ | setLpPair | External ❗ | " | | onlyOwner |

| └ | setInitializers | External ❗ | " | | onlyOwner |

| └ | isExcludedFromFees | External ❗ | | |NO❗ |

| └ | isExcludedFromDividends | External ❗ | | |NO❗ |

| └ | isExcludedFromProtection | External ❗ | | |NO❗ |

| └ | setDividendExcluded | Public ❗ | " | | onlyOwner |

| └ | setExcludedFromFees | Public ❗ | " | | onlyOwner |

OPTIMIZATIONS | AANN

ID	Title	Category	Status
CTV	Logarithm Refinement Optimization	Gas Optimization	Acknowledged
COP	Checks Can Be Performed Earlier	Gas Optimization	Acknowledged
CDP	Unnecessary Use Of SafeMath	Gas Optimization	Acknowledged
CWY	Struct Optimization	Gas Optimization	Acknowledged
CGT	Unused State Variable	Gas Optimization	Acknowledged

General Detectors

Transfer Limit

The max/min amount of token transferred can be limited (max could be set to 0).

Attention Required

DoS with Failed Call

This contract uses external calls that may fail, resulting in loss of functionality

Attention Required

Division Before Multiplication

The order of operations used may result in a loss of precision.

Attention Required

- No compiler version inconsistencies found
- No unchecked call responses found
- No vulnerable self-destruct functions found
- No assertion vulnerabilities found
- No old solidity code found
- No external delegated calls found
- No external call dependency found
- No vulnerable authentication calls found
- No invalid character typos found
- No RTL characters found
- No dead code found
- No risky data allocation found
- No uninitialized state variables found
- No uninitialized storage variables found
- No vulnerable initialization functions found
- No risky data handling found
- No number accuracy bug found
- No out-of-range number vulnerability found
- No map data deletion vulnerabilities found
- No tautologies or contradictions found
- No faulty true/false values found
- No innacurate divisions found
- No redundant constructor calls found
- No vulnerable transfers found
- No vulnerable return values found
- No uninitialized local variables found
- No default function responses found
- No missing arithmetic events found
- No missing access control events found
- No redundant true/false comparisons found
- No state variables vulnerable through function calls found
- No buggy low-level calls found
- No expensive loops found
- No bad numeric notation practices found
- No missing constant declarations found
- No missing external function declarations found
- No vulnerable payable functions found
- No vulnerable message values found

Vulnerability Run check

Risk Analysis

Contract source code verified

This token contract is open source. You can check the contract code for details. Unsourced token contracts are likely to have malicious functions to defraud their users of their assets.

No Proxy

There is no proxy in the contract. The proxy contract means contract owner can modify the function of the token and possibly effect the price.

No mint function

Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token.

No function to retrieve ownership

If this function exists, it is possible for the project owner to regain ownership even after relinquishing it.

Owner cant change balance

The contract owner does not have the authority to modify the balance of tokens at other addresses.

Honeypot Risk

This does not appear to be a honeypot

We are not aware of any code that prevents the sale of tokens.

No trading cooldown

The token contract has no trading cooldown function. If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying.

No Anti Whale

There is no limit to the number of token transactions. The number of scam token transactions may be limited (honeypot risk).

No blacklist function

No blacklist function is included.

No whitelist function

Whitelist function found

AN-01 Key Findings

Category	Severity	Target	Status
Business Logic	Medium	Contract/ANtoken.sol 400-402	Low

Description

In **updateForOwner**, Relevant Function Snippet

```
function allowance(address owner_, address spender_) external view returns (uint256) {
        return _allowances[owner_][spender_];
    }
```

Description

For Ownership efficiency, the **Ai Social Authenticity Network** Team is engineered with the reserve cache mechanism, which necessi-tates the common steps to be followed when operating with the reserve Ownership data in different scenarios, including the tax generation, update, and eventual persistence.

Recommendation

Revise the above functions to following a consistent approach to use the reserve cache mechanism.

AN-02 Key Findings

Category	Severity ●	Location	Status
Status Mathematical Operations	Low	Contract/ANTokenMultichain.sol 195-198	Informational

Description

In **UncheckedForTransfer ,** the following equation is used inside an unchecked block

```
        function transfer(address to_, uint256 amount_) external returns (bool) {
        _transfer(msg.sender, to_, amount_);
        return true;
    }
```

A transfer call made in this contract **might** be unstable and cause tokens to become stuck.

Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the **ANTokenMultichain** contract.

Recommendation

Incorporate the following verification within process approve account to confirm that the contract account's associated **transfer** aligns with the mint for which the confidential transfer approval is sought.

AN-03 POSSIBLE OVERFLOW

Category	Severity ●	Location	Status
Status Mathematical Operations	Minor	Contract/ANToken.sol	Acknowledged

Description

In **updateForMinter** , the following equation is used inside an unchecked block

```
function mint(address account_) external onlyRole(DEFAULT_ADMIN_ROLE) {
        if (account_ == address(0)) {
            revert ZeroAddressEntry();
        }
        if (isTradingEnabled) {
            revert ForbiddenToMintTokens();
        }
        unchecked {
            _totalSupply += MAXIMUM_SUPPLY;
            _balances[account_] += MAXIMUM_SUPPLY;
        }
```

Minter can not issue more **ANToken** indefinitely.

Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the **ANTOKEN** contract.

Recommendation

We recommend either checking for overflow in this case, or ensuring that the PairsIn is close enough it will never cause an overflow.

AN-04 Key Findings

Category	Severity ●	Target	Status
Inconsistency	Informational	Multiple Contracts	Acknowledge

Description

In **updateForAmount**, Relevant Function Snippet

```
function withdrawAccumulatedCommission() external onlyRole(DEFAULT_ADMIN_ROLE) {
        uint256 commissionAmount = _balances[address(this)];
        if (commissionAmount > 0) {
            _transfer(address(this), commissionRecipient, commissionAmount);
            emit AccumulatedCommissionWithdrawn(commissionAmount);
        }
    }
```

Description

The function **amount0**() does not have the override specifier. It should be noted that since **amount**0 > a function That overrides only a single interface function does not require the override specifier. However, all other instances of this in the codebase contain the override specifier.

Recommendation

We recommend adding the override specifier to **amount**() or removing the override specifier from all other functions this applies to for consistency.

Vulnerability Scan

REENTRANCY

No reentrancy risk found

Severity	Major
Confidence Parameter	Certain

Vulnerability Description

Mintable: More amount of the **ANtoken** can **NOT** be minted by a private wallet or contract. **(This is Essentially normal for most contracts)**

Scanning Line:

```
  function _mint(address account_, uint256 amount_) private {
        _totalSupply += amount_;
        uint256 adjustedAmount =
amount_.div(cumulativeAdjustmentFactor);
        if (_burnProtectedAccounts.contains(account_)) {
            _balances[account_] += amount_;
        } else {
            _balances[account_] += adjustedAmount;
        }
        emit Transfer(address(0), account_, amount_);
    }
```

Repository:

https://github.com/aann-ai

Audited Files

O.ANToken.sol
O.ANTokenMultichain.sol
O.IANToken.sol
O.IANTokenMultichain.sol
O.IWormholeReceiver.sol
0.IWormholeRelayer.sol

Contract Creator Address

Not Established

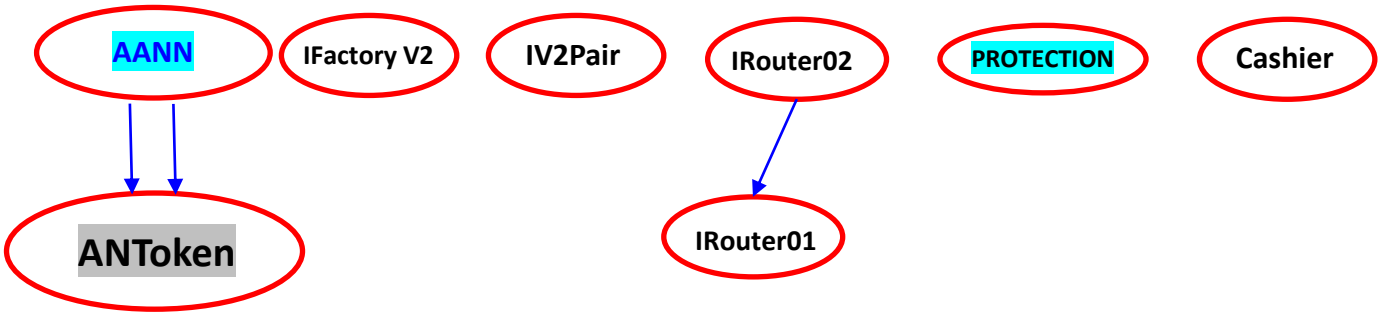
Deployed Contracts:

Not Deployed

Creator TXH Contracts:

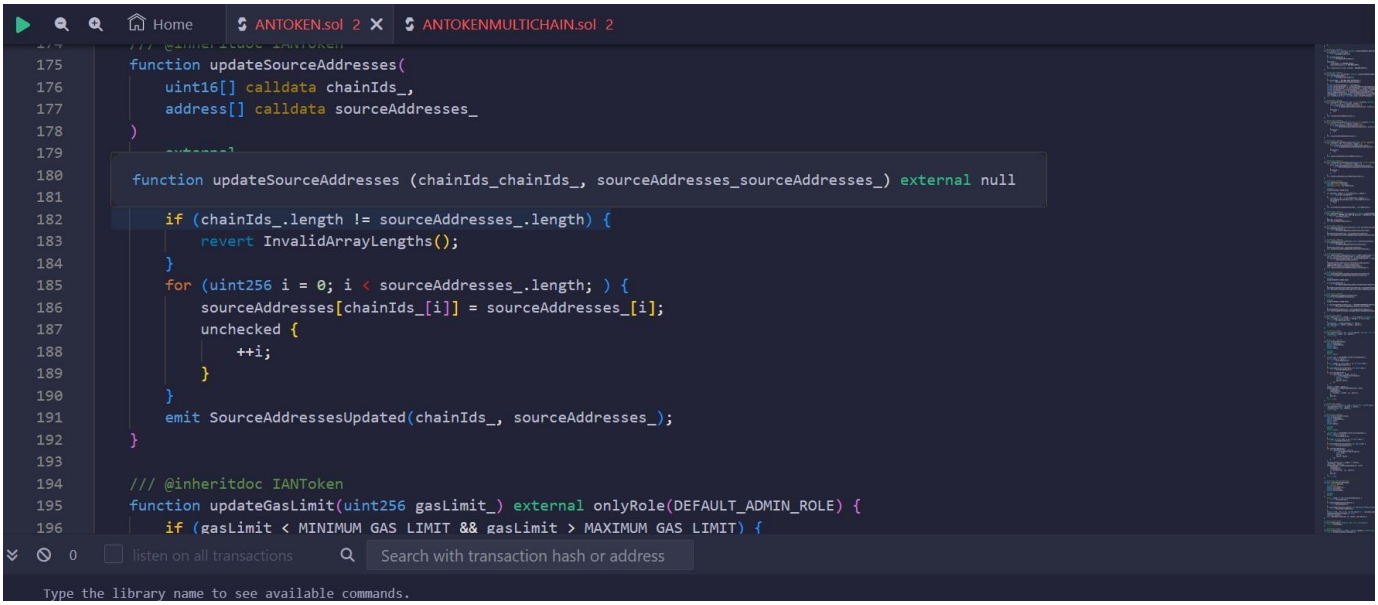
Not Refillable

INHERITANCE GRAPH



Identifier	Definition	Severity
CEN-12	Centralization privileges of AANN	Medium

Vulnerability 0 : No important security issue detected.
Threat level: Low



VitalBlock

ISSUES CHECKING STATUS

	Issue Description	Checking Status
1.	Compiler errors.	PASSED
2.	Race Conditions and reentrancy. Cross-Function Race Conditions.	PASSED
3.	Possible Delay In Data Delivery.	PASSED
4.	Oracle calls.	PASSED
5.	Front Running.	PASSED
6.	Sol. Dependency.	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.	The Impact Of Exchange Rate On the solidity Logic.	PASSED
13.	Private use data leaks.	PASSED
14.	Malicious Event log.	PASSED
15.	Scoping and Declarations.	PASSED
16.	Uninitialized storage pointers.	PASSED
17.	Arithmetic accuracy.	PASSED
18.	Design Logic.	PASSED
19.	Cross-Function race Conditions	PASSED
20.	Save Upon solidity contract Implementation and Usage.	PASSED
21.	Fallback Function Security	PASSED

AUDIT RESULT

PASSED

MANUAL REVIEW

What is Social Authenticity (#SocAuth) and why is it so important for online social media? Simply explained, social authenticity is the act of being true to one's representation in online social environments and presenting a genuine version of yourself, business, community or brand to the world, or to your followers. Our modern society is often plagued by information distortion, and superficiality. The need for social authenticity in online interactions is growing every year due to the ensuing social trust crisis.

With the rise of Artificial Intelligence in online social media, users are experiencing a growing need for trusted interactions, provable authenticity and realness. This is where we see the biggest shift is occurring, while it is important to note AI is playing an increasingly important role in ensuring online social authenticity as well. As the battle lines are drawn between AI for Good vs AI for social manipulation, this is a "war" that AN plans to help our users WIN!

The Ai Social Authenticity Network Platform Is Launching Soon.

Identifier	Definition	Severity
CEN-02	Initial asset distribution	Minor

All of the initially minted assets are sent to the contract deployer when deploying the contract. This is Normal for most deployer and/or contract owner .

```
function approve(address spender_, uint256 amount_) external returns (bool) {
        if (msg.sender == address(0) || spender_ == address(0)) {
            revert ZeroAddressEntry();
        }
        _allowances[msg.sender][spender_] = amount_;
        emit Approval(msg.sender, spender_, amount_);
        return true;
    }
```

RECOMMENDATION

Project stakeholders should be consulted during the initial asset distribution process.

RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully.

Please refer to PAGE-7 CENTRALIZED PRIVILEGES for a detailed understanding.

ALLEVIATION

The AANN project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behavior in the project

References

1 MITRE. CWE-1041: Use of Redundant Code. https://cwe.mitre.org/data/definitions/1041.html.

2 MITRE. CWE-1099: Inconsistent Naming Conventions for Identifiers. https://cwe.mitre.org/data/definitions/1099.html.

3 MITRE. CWE-561: Dead Code. https://cwe.mitre.org/data/definitions/561.html.

4 MITRE. CWE-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

5 MITRE. CWE-663: Use of a Non-reentrant Function in a Concurrent Context. https://cwe.mitre.org/data/definitions/663.html.

6 MITRE. CWE-837: Improper Enforcement of a Single, Unique Action. https://cwe.mitre.org/data/definitions/837.html.

7 MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

8 MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

9 MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

10 MITRE. CWE CATEGORY: Concurrency. https://cwe.mitre.org/data/definitions/557.html.

11 MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

12 OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

Identifier	Definition	Severity
COD-10	Third Party Dependencies	Minor

Smart contract is interacting with third party protocols e.g., Pancakeswap router, cashier contract, protections contract. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised, and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.

DISCLAIMERS

Vital Block Security provides the easy-to-understand audit of Solidity, Move and Raw source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way

to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, VITAL BLOCK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT'S OR ANY OTHER INDIVIDUAL'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. Vital Block does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.

LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than Vital Block. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites and social accounts owners. You agree that Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.

ABOUT VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 50+ smart contracts, and analyzed 200,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: https://Vitalblock.org

Email: info@vitalblock.org

GitHub: https://github.com/vital-block

Telegram (Engineering): https://t.me/vital_block

Telegram (Onboarding): https://t.me/vitalblock_cmo

vital-block

info@vitalblock.org

www.Vitalblock.org

Vital Block Dedicated to securing Public and Private Blockchain Ecosystem