



CFG NINJA AUDITS

Security Assessment

Altom Token

July 19, 2023

Audit Status: Pass











Audit Edition: Advanced

Risk Analysis


















Classifications of Manual Risk Results

| Classification | Description |
|---|----------------------------------|
|  Critical | Danger or Potential Problems. |
|  High | Be Careful or Fail test. |
|  Low | Pass, Not-Detected or Safe Item. |
|  Informational | Function Detected |

Manual Code Review Risk Results

| Contract Privilege | Description |
|--|--------------|
|  Buy Tax | 0% |
|  Sale Tax | 10% |
|  Cannot Sale | Pass |
|  Cannot Sale | Pass |
|  Max Tax | 15% |
|  Modify Tax | No |
|  Fee Check | Pass |
|  Is Honeygot? | Not Detected |
|  Trading Cooldown | Not Detected |
|  Can Pause Trade? | Not Detected |



| Contract Priviledge | Description |
|--|--|
|  Pause Transfer? | Not Detected |
|  Max Tx? | Pass |
|  Is Anti Whale? | Not Detected |
|  Is Anti Bot? | Not Detected |
|  Is Blacklist? | Not Detected |
|  Blacklist Check | Pass |
|  is Whitelist? | Detected |
|  Can Mint? | Pass |
|  Is Proxy? | Not Detected |
|  Can Take Ownership? | Not Detected |
|  Hidden Owner? | Not Detected |
|  Owner | 0xa984f00690ac3d79d07400a4bd065c15d91816df |
|  Self Destruct? | Not Detected |
|  External Call? | Not Detected |
|  Other? | Not Detected |
|  Holders | 1 |
|  Auditor Confidence | Medium |

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Project Overview

Token Summary

| Parameter | Result |
|---------------|---|
| Address | 0x9578A9937dFf45b4E29e49120AB83cb806f1aa4F |
| Name | AITom |
| Token Tracker | AITom (AITom) |
| Decimals | 18 |
| Supply | 100,000,000,000 |
| Platform | Arbitrium |
| compiler | v0.8.4+commit.c7e474f2 |
| Contract Name | AiTomToken |
| Optimization | Yes with 200 runs |
| LicenseType | MIT |
| Language | Solidity |
| Codebase | https://arbiscan.io/address/0x9578a9937dff45b4e29e49120ab83cb806f1aa4f#code |
| Payment Tx | Corporate |



Main Contract Assessed Contract Name

| Name | Contract | Live |
|-------|--|------|
| AITom | 0x9578A9937dFf45b4E29e49120AB83cb806f1aa4F | Yes |

TestNet Contract Assessed Contract Name

| Name | Contract | Live |
|-------|--|------|
| AITom | 0xa899CbBddE23fba859cea7d17442c9e30017d017 | Yes |

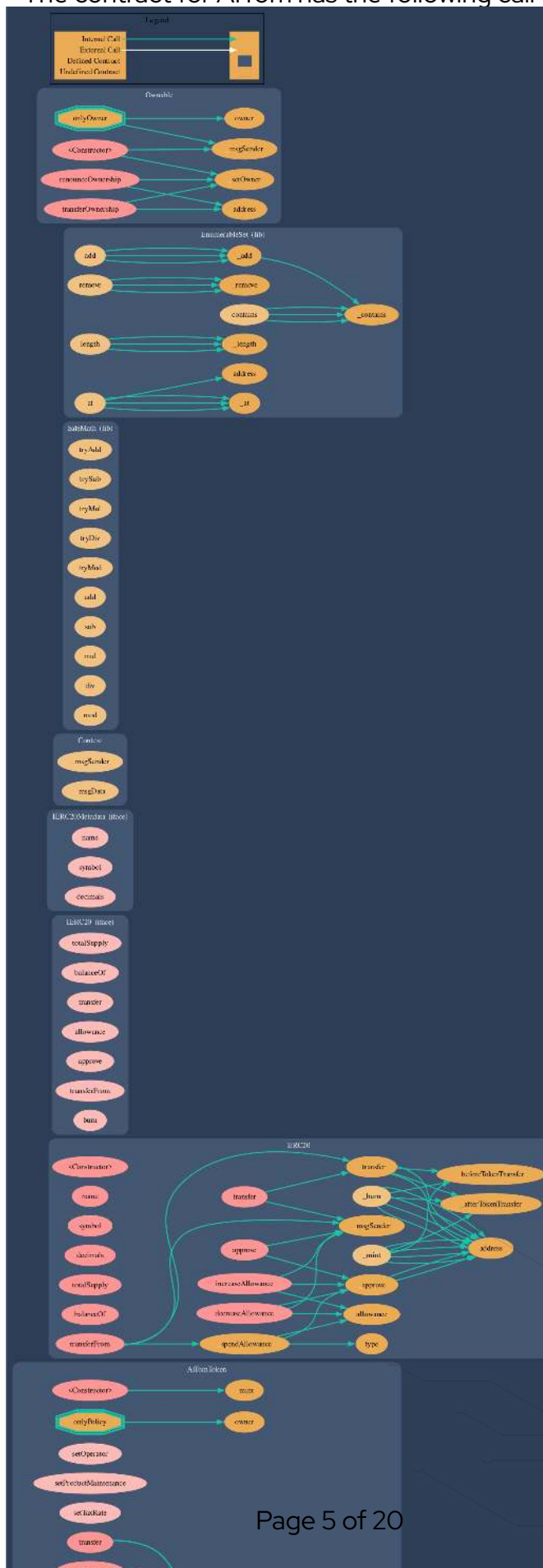
Solidity Code Provided

| SolID | File Sha-1 | FileName |
|-------|--|--------------------|
| AiTom | 30fb0b9ae53f724bea6e2e36bab8e93bacc20a0a | AiTomToken.sol |
| AiTom | b966b2bcd608732e1d34c762af10b2afa943a4e | ERC20.sol |
| AiTom | a9f5317adce9581ccdface9d1ffa8b3a3391560b | IERC20.sol |
| AiTom | b592b692485ad10f8ec55476dd3fcdcc51e0f62c | IERC20Metadata.sol |



Call Graph

The contract for AlTom has the following call graph structure.



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

| ID | Severity | Name | File | location |
|---------|----------|---|----------------|-----------|
| SWC-100 | Pass | Function Default Visibility | AiTomToken.sol | L: 0 C: 0 |
| SWC-101 | Pass | Integer Overflow and Underflow. | AiTomToken.sol | L: 0 C: 0 |
| SWC-102 | Pass | Outdated Compiler Version file. | AiTomToken.sol | L: 0 C: 0 |
| SWC-103 | Pass | A floating pragma is set. | AiTomToken.sol | L: 0 C: 0 |
| SWC-104 | Pass | Unchecked Call Return Value. | AiTomToken.sol | L: 0 C: 0 |
| SWC-105 | Pass | Unprotected Ether Withdrawal. | AiTomToken.sol | L: 0 C: 0 |
| SWC-106 | Pass | Unprotected SELFDESTRUCT Instruction | AiTomToken.sol | L: 0 C: 0 |
| SWC-107 | Pass | Read of persistent state following external call. | AiTomToken.sol | L: 0 C: 0 |
| SWC-108 | Pass | State variable visibility is not set.. | AiTomToken.sol | L: 0 C: 0 |
| SWC-109 | Pass | Uninitialized Storage Pointer. | AiTomToken.sol | L: 0 C: 0 |
| SWC-110 | Pass | Assert Violation. | AiTomToken.sol | L: 0 C: 0 |



| ID | Severity | Name | File | location |
|---------|----------|--|----------------|-----------|
| SWC-111 | Pass | Use of Deprecated Solidity Functions. | AiTomToken.sol | L: 0 C: 0 |
| SWC-112 | Pass | Delegate Call to Untrusted Callee. | AiTomToken.sol | L: 0 C: 0 |
| SWC-113 | Pass | Multiple calls are executed in the same transaction. | AiTomToken.sol | L: 0 C: 0 |
| SWC-114 | Pass | Transaction Order Dependence. | AiTomToken.sol | L: 0 C: 0 |
| SWC-115 | Pass | Authorization through tx.origin. | AiTomToken.sol | L: 0 C: 0 |
| SWC-116 | Pass | A control flow decision is made based on The block.timestamp environment variable. | AiTomToken.sol | L: 0 C: 0 |
| SWC-117 | Pass | Signature Malleability. | AiTomToken.sol | L: 0 C: 0 |
| SWC-118 | Pass | Incorrect Constructor Name. | AiTomToken.sol | L: 0 C: 0 |
| SWC-119 | Pass | Shadowing State Variables. | AiTomToken.sol | L: 0 C: 0 |
| SWC-120 | Pass | Potential use of block.number as source of randommness. | AiTomToken.sol | L: 0 C: 0 |
| SWC-121 | Pass | Missing Protection against Signature Replay Attacks. | AiTomToken.sol | L: 0 C: 0 |
| SWC-122 | Pass | Lack of Proper Signature Verification. | AiTomToken.sol | L: 0 C: 0 |
| SWC-123 | Pass | Requirement Violation. | AiTomToken.sol | L: 0 C: 0 |
| SWC-124 | Pass | Write to Arbitrary Storage Location. | AiTomToken.sol | L: 0 C: 0 |
| SWC-125 | Pass | Incorrect Inheritance Order. | AiTomToken.sol | L: 0 C: 0 |



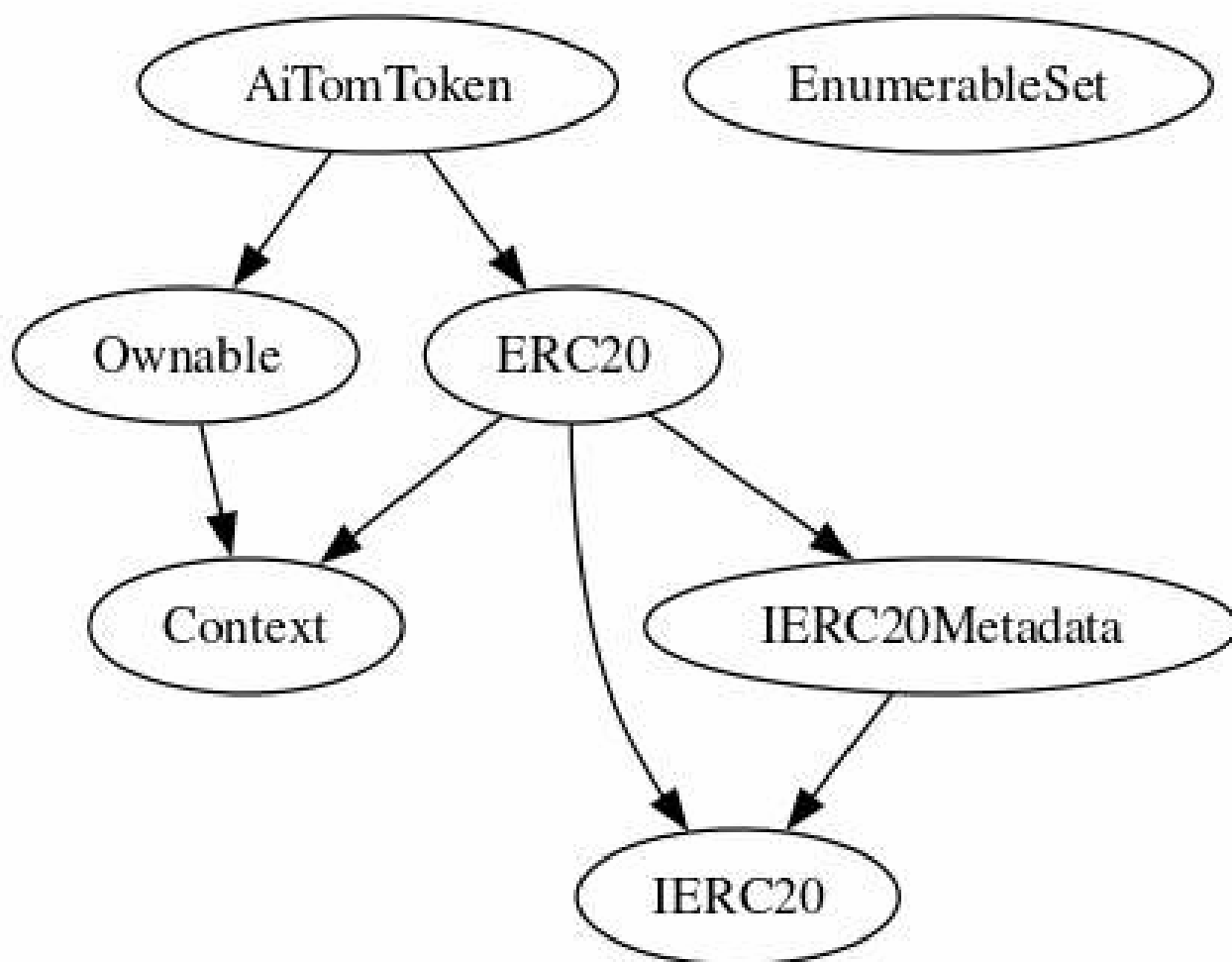
| ID | Severity | Name | File | location |
|---------|----------|--|----------------|-----------|
| SWC-126 | Pass | Insufficient Gas Griefing. | AiTomToken.sol | L: 0 C: 0 |
| SWC-127 | Pass | Arbitrary Jump with Function Type Variable. | AiTomToken.sol | L: 0 C: 0 |
| SWC-128 | Pass | DoS With Block Gas Limit. | AiTomToken.sol | L: 0 C: 0 |
| SWC-129 | Pass | Typographical Error. | AiTomToken.sol | L: 0 C: 0 |
| SWC-130 | Pass | Right-To-Left-Override control character (U+202E). | AiTomToken.sol | L: 0 C: 0 |
| SWC-131 | Pass | Presence of unused variables. | AiTomToken.sol | L: 0 C: 0 |
| SWC-132 | Pass | Unexpected Ether balance. | AiTomToken.sol | L: 0 C: 0 |
| SWC-133 | Pass | Hash Collisions with Multiple Variable Length Arguments. | AiTomToken.sol | L: 0 C: 0 |
| SWC-134 | Pass | Message call with hardcoded gas amount. | AiTomToken.sol | L: 0 C: 0 |
| SWC-135 | Pass | Code With No Effects (Irrelevant/Dead Code). | AiTomToken.sol | L: 0 C: 0 |
| SWC-136 | Pass | Unencrypted Private Data On-Chain. | AiTomToken.sol | L: 0 C: 0 |

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.



Inheritance

The contract for AiTom has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

| Function Name | Parameters | Visibility |
|----------------------------------|------------------|------------|
| renounceOwnership | | Public |
| transferOwnership | address newOwner | Public |
| addOremoveRecipie ntWhitelist | | External |
| addOremoveSender Whitelis | | External |
| caddOremoveTeamli st | | Public |
| setRate | | public |
| setInsuredPool | | External |
| setProductMaintena nce | | External |
| setEcologicalPromot er | | External |
| setOperator | | External |



Smart Contract Advance Checks



| ID | Severity | Name | Result | Status |
|----------|---------------|--|--------|--------------|
| AlTom-01 | Low | Potential Sandwich Attacks. | Pass | Not Detected |
| AlTom-02 | Informational | Function Visibility Optimization | Pass | Not Detected |
| AlTom-03 | Low | Lack of Input Validation. | Pass | Not Detected |
| AlTom-04 | High | Centralized Risk In addLiquidity. | Pass | Not Detected |
| AlTom-05 | Low | Missing Event Emission. | Pass | Not Detected |
| AlTom-06 | Low | Conformance with Solidity Naming Conventions. | Pass | Not Detected |
| AlTom-07 | Low | State Variables could be Declared Constant. | Pass | Not Detected |
| AlTom-08 | Low | Dead Code Elimination. | Pass | Not Detected |
| AlTom-09 | High | Third Party Dependencies. | Pass | Not Detected |
| AlTom-10 | High | Initial Token Distribution. | Pass | Not Detected |
| AlTom-11 | High | claimStuckTokens can claim own tokens. | Pass | Not Detected |
| AlTom-12 | High | Centralization Risks In The X Role | Pass | Not Detected |
| AlTom-13 | Informational | Extra Gas Cost For User.. | Fail | Detected |
| AlTom-14 | Medium | Unnecessary Use Of SafeMath | Pass | Not Detected |
| AlTom-15 | Medium | Symbol Length Limitation due to Solidity Naming Standards. | Pass | Not Detected |



| ID | Severity | Name | Result | Status |
|----------|---------------|--|--------|--------------|
| AITom-16 | Medium | Taxes can be up to 100% | Pass | Not Detected |
| AITom-17 | Logical Issue | Highly Permissive Role Access, | Pass | Not Detected |
| AITom-18 | Critical | Stop Transactions by using Enable Trade. | Pass | Not Detected |



AITom-13 | Extra Gas Cost For User.

| Category | Severity | Location | Status |
|---------------|---|------------------------------|--|
| Logical Issue |  Informational | AiTomToken.sol: L: 264, C: 0 |  Detected |

Description

The user may trigger a tax distribution during the transfer process, which will cost a lot of gas and it is unfair to let a single user bear it.

Remediation

We advise the client to make the owner responsible for the gas costs of the tax distribution.

Project Action








Technical Findings Summary

Classification of Risk

| Severity | Description |
|---|--|
|  Critical | Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks. |
|  High | Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project. |
|  Medium | Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform |
|  Low | Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions. |
|  Informational | Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code. |

Findings

| Severity | Found | Pending | Resolved |
|---|-------|---------|----------|
|  Critical | 0 | 0 | 0 |
|  High | 0 | 0 | 0 |
|  Medium | 0 | 0 | 0 |
|  Low | 0 | 0 | 0 |
|  Informational | 1 | 0 | 0 |
| Total | 1 | 0 | 0 |



Social Media Checks

| Social Media | URL | Result |
|--------------|---|--------|
| Twitter | https://twitter.com/MemeAitom | Pass |
| Other | | Fail |
| Website | https://aitom.pro/ | Pass |
| Telegram | https://t.me/AITomPro | Pass |

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Assessment Results

Score Results

| Review | Score |
|---------------------|--------|
| Overall Score | 91/100 |
| Auditor Score | 95/100 |
| Review by Section | Score |
| Manual Scan Score | 19/33 |
| SWC Scan Score | 37 /37 |
| Advance Check Score | 35 /30 |

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed



Assessment Results

Important Notes:

- The team has performed the necessary coding changes to pass the audit.
- The token was tested using PCS and did not find any problems, however, keep in mind that our simulations are limited to basic actions.
- Please DYOR on the project.

Auditor Score =95
Audit Passed



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how `block.timestamp` works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.



Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.



Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access 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. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

