



Full Audit Report

AIMEME Security Assessment

Real Cybersecurity
Protecting digital assets



Made in Thailand

SECURI LAB
(THAILAND) contact@securi-lab.com



Audit



FULL AUDIT REPORT

Table of Contents	1
▪ Report Information	2
▪ Disclaimer	3
▪ Executive Summary	4
NVD CVSS Scoring	
Audit Result	
▪ Project Introduction	5
Scope Information	
Audit Information	
Audit Version History	
▪ Initial Audit Scope	6-7
▪ Security Assessment Procedure	8
▪ Risk Rating	9
▪ Vulnerability Severity Summary	10
▪ Vulnerability Findings	11-18
SWC & SEC & Non-severity level	
▪ SWC Findings	19-21
▪ Visibility, Mutability, Modifier function testing	22-27
Component, Exposed Function	
StateVariables, Capabilities, Contract Descripton Table	
▪ Inheritate Function Relation Graph	28
▪ UML Diagram	29
▪ About SECURI LAB	30

FULL AUDIT REPORT

Report Information

About Report	AIMEME Security Assessment
Version	v1.2
Client	AIMEME
Language	Solidity
Confidentiality	Public
Contract File / Contract Address	0xfd124A610Ae299E574A83fbF3738dB75DB1D751d
Audit Method	Whitebox
Security Assessment Author	<p>Auditor </p> <p>Mark K. [Security Researcher Redteam] Kevin N. [Security Researcher Web3 Dev] Yusheng T. [Security Researcher Incident Response]</p> <p>Approve Document</p> <p>Ronny C. CTO & Head of Security Researcher Chinnakit J. CEO & Founder</p>

*Audit Method

Whitebox: SECURI LAB Team receives all source code from the client to provide the assessment.

Blackbox: SECURI LAB Team receives only bytecode from the client to provide the assessment.

Digital Sign (Only Full Audit Report)

FULL AUDIT REPORT

Disclaimer

Regarding this security assessment, there are no guarantees about the security of the program instruction received from the client is hereinafter referred to as **"Source code"**.

And **SECURI Lab** hereinafter referred to as **"Service Provider"**, the **Service Provider** will not be held liable for any legal liability arising from errors in the security assessment. The responsibility will be the responsibility of the **Client**, hereinafter referred to as **"Service User"** and the **Service User** agrees not to be held liable to the **service provider** in any case. By contract **Service Provider** to conduct security assessments with integrity with professional ethics, and transparency to deliver security assessments to users The **Service Provider** has the right to postpone the delivery of the security assessment. If the security assessment is delayed whether caused by any reason and is not responsible for any delayed security assessments.

If the **service provider** finds a vulnerability The **service provider** will notify the **service user** via the Preliminary Report, which will be kept confidential for security. The **service provider** disclaims responsibility in the event of any attacks occurring whether before conducting a security assessment. Or happened later All responsibility shall be sole with the **service user**.

Security Assessment Not Financial/Investment Advice Any loss arising from any investment in any project is the responsibility of the investor.

SECURI LAB disclaims any liability incurred. Whether it's Rugpull, Abandonment, Soft Rugpull, Exploit, Exit Scam.



The SECURI LAB team has conducted a comprehensive security assessment of the vulnerabilities. This assessment is tested with an expert assessment. Using the following test requirements

1. Smart Contract Testing with Expert Analysis By testing the most common and uncommon vulnerabilities.
2. Automated program testing It includes a sample vulnerability test and a sample of the potential vulnerabilities being used for the most frequent attacks.
3. Manual Testing with AST/WAS/ASE/SMT and reviewed code line by line
4. Visibility, Mutability, Modifier function testing, such as whether a function can be seen in general, or whether a function can be changed and if so, who can change it.
5. Function association test It will be displayed through the association graph.
6. This safety assessment is cross-checked prior to the delivery of the assessment results.

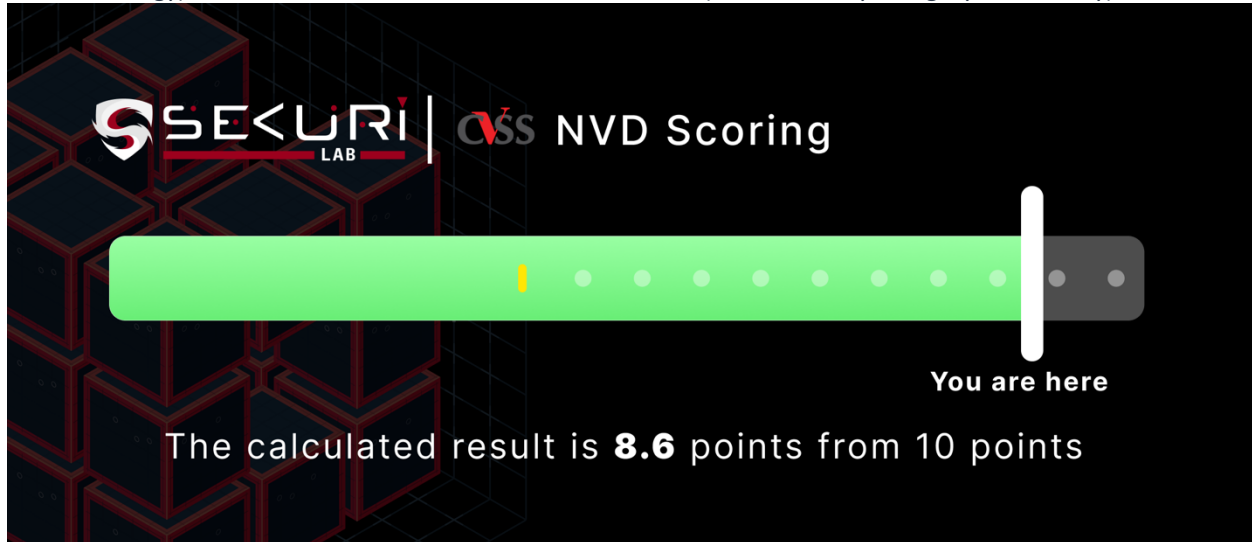
FULL AUDIT REPORT

Executive Summary

For this security assessment, SECURI LAB received a request from AIMEME on Thursday, June 29, 2023.

NVD CVSS Scoring

The score was calculated using the NVD (National Vulnerability Database) of NIST (National Institute of Standards and Technology) under the CVSS 3.1 standard, based on the CIA (Confidentiality, Integrity, Availability).



Audit Result

SECURI LAB evaluated the smart contract security of the project and found: **[Total : 5]**

Critical	High	Medium	Low	Very Low	Informational
0	1	2	0	0	2



SECURI LAB has assessed the security of this smart contract.

The results of the security assessment revealed

No Critical Vulnerabilities.

Full Audit Report by SECURI LAB on July 25, 2023



FULL AUDIT REPORT

Project Introduction

Scope Information:

Project Name	AIMEME
Website	https://aimeme.ai/
Chain	Ethereum Mainnet
Language	Solidity

Audit Information:

Request Date	Thursday, June 29, 2023
Audit Date	Monday, July 3, 2023
Re-assessment Date	Monday, July 24, 2023

Audit Version History:

Version	Date	Description
1.0	Monday, July 3, 2023	Preliminary Report
1.1	Monday, July 24, 2023	Preliminary Report With Re-Assessment
1.2	Wednesday, July 26, 2023	Full Audit Report

FULL AUDIT REPORT

Initial Audit Scope:

Smart Contract File	AIMToken.sol SHA-1: 58d5f04499af69fa24d7a44b036800a56b854d00
This audit uses the file as the client submitted. Please check with a differential checker after the smart contract code has been deployed and verified.	
Compiler Version	v0.8.9

Re-assessment Audit Scope:

Smart Contract File	0xfd124A610Ae299E574A83fbF3738dB75DB1D751d
Compiler Version	v0.8.9+commit.e5eed63a

Source Units Analyzed: 1

Source Units in Scope: 1 (100%)

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	AIMToken.sol	4	4	1041	893	477	387	328	Σ
	Totals	4	4	1041	893	477	387	328	Σ

Legend: []

- **Lines:** total lines of the source unit
- **nLines:** normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC:** normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines:** lines containing single or block comments
- **Complexity Score:** a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

FULL AUDIT REPORT

Dependencies / External Imports

Dependency / Import Path	Count
@chainlink/contracts/src/v0.8/interfaces/AggregatorV3Interface.sol	1
@openzeppelin/contracts/access/Ownable.sol	1
@openzeppelin/contracts/token/ERC20/ERC20.sol	1



FULL AUDIT REPORT

Security Assessment Procedure

Securi has the following procedures and regulations for conducting security assessments:

1.Request Audit Client submits a form request through the Securi channel. After receiving the request, Securi will discuss a security assessment. And drafting a contract and agreeing to sign a contract together with the Client

2.Auditing Securi performs security assessments of smart contracts obtained through automated analysis and expert manual audits.

3.Preliminary Report At this stage, Securi will deliver an initial security assessment. To report on vulnerabilities and errors found under Audit Scope will not publish preliminary reports for safety.

4.Reassessment After Securi has delivered the Preliminary Report to the Client, Securi will track the status of the vulnerability or error, which will be published to the Final Report at a later date with the following statuses:

a.Acknowledge The client has been informed about errors or vulnerabilities from the security assessment.

b.Resolved The client has resolved the error or vulnerability. Resolved is probably just a commit, and Securi is unable to verify that the resolved has been implemented or not.

c.Decline Client has rejected the results of the security assessment on the issue.

5.Final Report Securi providing full security assessment report and public



FULL AUDIT REPORT

Risk Rating

Risk rating using this commonly defined: $Risk\ rating = impact * confidence$

Impact The severity and potential impact of an attacker attack

Confidence Ensuring that attackers expose and use this vulnerability

Both have a total of 3 levels: **High, Medium, Low**. By *Informational* will not be classified as a level

Confidence Impact [Likelihood]	Low	Medium	High
Low	Very Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical



FULL AUDIT REPORT

Vulnerability Severity Summary

Severity is a risk assessment It is calculated from the Impact and Confidence values using the following calculation methods,

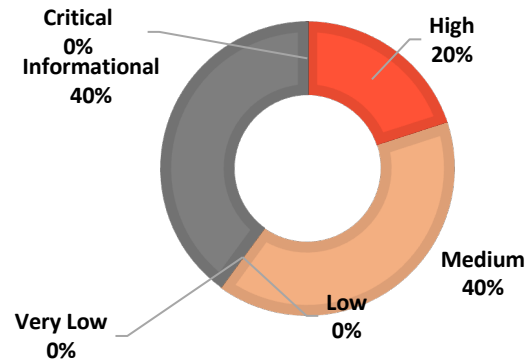
$$\text{Risk rating} = \text{impact} * \text{confidence}$$

It is categorized into

5 categories based on the lowest severity:

Very Low, Low, Medium, High, Critical.

For **Informational** & will **Non-class/Optimization/Best-practices** will not be counted as severity



Vulnerability Severity Level	Total
Critical	0
High	1
Medium	2
Low	0
Very Low	0
Informational	2
Non-class/Optimization/Best-practices	1

Category information:

Centralization Centralization Risk is The risk incurred by a sole proprietor, such as the Owner being able to change something without permission	Economics Risk Economics Risk is Risks that may affect the economic mechanism system, such as the ability to increase Mint token	Logical Issue Logical Issue is that can cause errors to core processing, such as any prior operations that cause background processes to crash.	Authorization Authorization is Possible pitfalls from weak coding allows unrelated people to take any action to modify the values.	Mathematical Mathematical Any erroneous arithmetic operations affect the operation of the system or lead to erroneous values.	Naming Conventions Naming Conventions naming variables that may affect code understanding or naming inconsistencies
Security Risk Security Risk of loss or damage if it's no mitigate	Coding Style Coding Style is Tips coding for efficiency performance	Best Practices Best Practices is suggestions for improvement	Optimization Optimization is performance improvement	Gas Optimization Gas Optimization is increase performance to avoid expensive gas	Dead Code Dead Code having unused code This may result in wasted resources and gas fees.

FULL AUDIT REPORT

Vulnerability Findings

ID	Vulnerability Detail	Severity	Category	Status
SEC-01	Centralization Risk	High	Centralization	Acknowledge
SEC-02	Imprecise arithmetic operations order (divide-before-multiply)	Medium	Best Practices	Resolved
SEC-03	Tautology or contradiction (tautology)	Medium	Best Practices	Resolved
SEC-04	Detects functions with high (> 11) cyclomatic complexity (cyclomatic-complexity)	Informational	Best Practices	Acknowledge
SEC-05	Unlocked pragma	Informational	Best Practices	Resolved
GAS-01	Use Custom Errors	-	Gas Optimization	Resolved



FULL AUDIT REPORT

SEC-01: Centralization Risk

Vulnerability Detail	Severity	Location	Category	Status
Centralization Risk	High	Check on finding	Centralization	Acknowledge

Finding:

```
30: contract AIMToken is ERC20, Ownable {  
  
95:     function startTheSale() public onlyOwner {  
  
295:     function withdraw() public onlyOwner {  
  
303:     function withdrawUSDT(uint256 _amount) public onlyOwner {  
  
...}
```

Explain Function Capability:

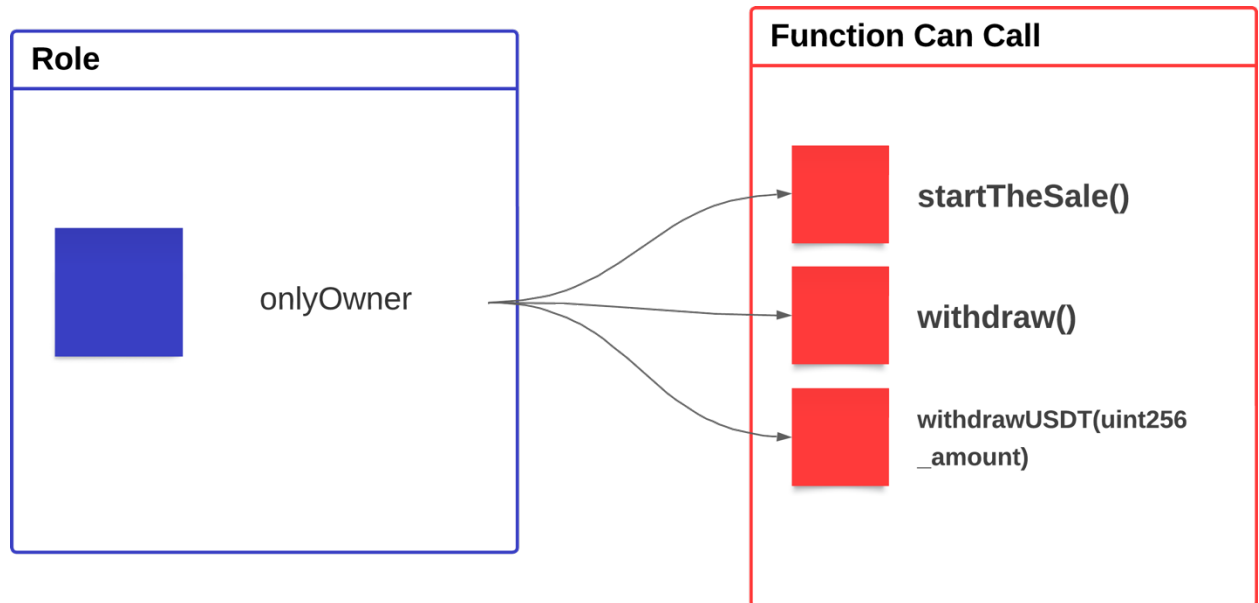
The contract provides several functions:

- **startTheSale()**: This function is a public function that can only be called by the contract owner. Its purpose is to start the token sale by incrementing the **round** variable. The **round** variable represents the current round of the token sale, and it is initially set to 0. By calling **startTheSale()**, the owner can increment the **round** variable to start the next round of the sale. The function checks if all rounds have been finished ($\text{round} < 6$) before incrementing the **round** variable.
- **withdraw()**: This function is a public function that can only be called by the contract owner. Its purpose is to **withdraw the Ether balance from the contract**. When called, the function transfers the entire balance of the contract to the address of the owner. The function uses the **call** function to send the Ether and checks the return value to ensure the transfer was successful. If the transfer fails, it reverts with the **transferFailed()** error.
- **withdrawUSDT(uint256 _amount)**: This function is a public function that can only be called by the contract owner. Its purpose is to **withdraw USDT tokens from the contract**. The function takes an input parameter **_amount**, which represents the amount of USDT tokens to be withdrawn. The function transfers the specified amount of USDT tokens from the contract to the owner's address using the **transfer** function of the **IERC20USDT** interface. It checks the balance of the contract to ensure it has enough USDT tokens before performing the transfer. If the contract doesn't have enough USDT tokens, it reverts with the **contractDontHaveUSDT()** error.

Please check to **Contracts Description Table** section to see full table of contract

FULL AUDIT REPORT

Centralization Risk Contract AIMToken (File: AIMToken.sol)



In the AIMToken contract, Owner can call functions **startTheSale()**, **withdraw()**, **withdrawUSDT(uint256 _amount)**.



Recommendation:

In terms of timeframes, there are three categories: short-term, long-term, and permanent.

For short-term solutions, a combination of timelock and multi-signature (2/3 or 3/5) can be used to mitigate risk by delaying sensitive operations and avoiding a single point of failure in key management. This includes implementing a timelock with a reasonable latency, such as 48 hours, for privileged operations; assigning privileged roles to multi-signature wallets to prevent private key compromise; and sharing the timelock contract and multi-signer addresses with the public via a medium/blog link.

For long-term solutions, a combination of timelock and DAO can be used to apply decentralization and transparency to the system. This includes implementing a timelock with a reasonable latency, such as 48 hours, for privileged operations; introducing a DAO/governance/voting module to increase transparency and user involvement; and sharing the timelock contract, multi-signer addresses, and DAO information with the public via a medium/blog link.

Finally, permanent solutions should be implemented to ensure the ongoing security and protection of the system.

Alleviation:

AIMEME has acknowledge this issue.

FULL AUDIT REPORT

SEC-02: Imprecise arithmetic operations order (divide-before-multiply)

Vulnerability Detail	Severity	Location	Category	Status
Imprecise arithmetic operations order (divide-before-multiply)	Medium	Check on finding	Best Practices	Resolved

Finding:

```

X AIMToken.sellTokenInETHPrice(uint256,uint256) (AIMToken.sol:331-343) performs a
multiplication on the result of a division:
    • tokensAmountPrice = ((conversion * _amount) / 10 ** 18) / 10 ** 12
(AIMToken.sol#336-337)
    • amountInEthers = tokensAmountPrice * conversionRate (AIMToken.sol#338)
  
```

Recommendation:

Recommendation: Consider ordering multiplication before division.

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply>



Alleviation:

AIMEME has resolved this issue.

FULL AUDIT REPORT

SEC-03: Tautology or contradiction (tautology)

Vulnerability Detail	Severity	Location	Category	Status
Tautology or contradiction (tautology)	Medium	Check on finding	Best Practices	Resolved

Finding:

✗ `AIMToken.withdrawUSDT(uint256)` (`AIMToken.sol:303-309`) contains a tautology or contradiction:

- `USDTtoken.balanceOf(msg.sender) < 0` (`AIMToken.sol#304`)

Recommendation:

Recommendation: Fix the incorrect comparison by changing the value type or the comparison.

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#tautology-or-contradiction>

Alleviation:

AIMEME has resolved this issue.



FULL AUDIT REPORT

SEC-04: Detects functions with high (> 11) cyclomatic complexity (cyclomatic-complexity)

Vulnerability Detail	Severity	Location	Category	Status
Detects functions with high (> 11) cyclomatic complexity (cyclomatic-complexity)	Informational	Check on finding	Best Practices	Acknowledge

Finding:

✗ `AIMToken.mintByEth(uint256)` (`AIMToken.sol:207-282`) has a high cyclomatic complexity (14).

✗ `AIMToken.mintByUSDT(uint256)` (`AIMToken.sol:102-204`) has a high cyclomatic complexity (13).

Recommendation:

Recommendation: Reduce cyclomatic complexity by splitting the function into several smaller subroutines.

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#cyclomatic-complexity>



Alleviation:

AIMEME has acknowledge this issue.

FULL AUDIT REPORT

SEC-05: Unlocked pragma

Vulnerability Detail	Severity	Location	Category	Status
Unlocked pragma	Informational	Check on finding	Best Practices	Resolved

Finding:

```
2: pragma solidity ^0.8.9;
```

Recommendation:

Consider locking the compiler version if possible to prevent unexpected behavior.

Alleviation:

AIMEME has resolved this issue.



FULL AUDIT REPORT

GAS-01: Use Custom Errors

Vulnerability Detail	Severity	Location	Category	Status
Use Custom Errors	-	Check on finding	Gas Optimization	Resolved

Finding:

```
96:         require(round < 6, "All rounds are finished");

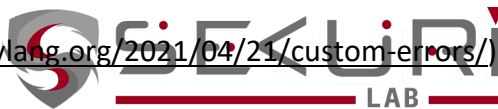
290:         require(price > 0, "Invalid USDT price"); // Ensure that the price is
valid

313:         require(round == 6, "please wait for preSale end");
```

Recommendation:

Instead of using error strings, to reduce deployment and runtime cost, you should use Custom Errors. This would save both deployment and runtime cost.

[Source](<https://blog.soliditylang.org/2021/04/21/custom-errors/>)

**Alleviation:**

AIMEME has resolved this issue.

FULL AUDIT REPORT

SWC Findings

ID	Title	Scanning	Result
SWC-100	Function Default Visibility	Complete	No risk
SWC-101	Integer Overflow and Underflow	Complete	No risk
SWC-102	Outdated Compiler Version	Complete	No risk
SWC-103	Floating Pragma	Complete	No risk
SWC-104	Unchecked Call Return Value	Complete	No risk
SWC-105	Unprotected Ether Withdrawal	Complete	No risk
SWC-106	Unprotected SELFDESTRUCT Instruction	Complete	No risk
SWC-107	Reentrancy	Complete	No risk
SWC-108	State Variable Default Visibility	Complete	No risk
SWC-109	Uninitialized Storage Pointer	Complete	No risk
SWC-110	Assert Violation	Complete	No risk
SWC-111	Use of Deprecated Solidity Functions	Complete	No risk
SWC-112	Delegatecall to Untrusted Callee	Complete	No risk
SWC-113	DoS with Failed Call	Complete	No risk
SWC-114	Transaction Order Dependence	Complete	No risk
SWC-115	Authorization through tx.origin	Complete	No risk

FULL AUDIT REPORT

SWC-116	Block values as a proxy for time	Complete	No risk
SWC-117	Signature Malleability	Complete	No risk
SWC-118	Incorrect Constructor Name	Complete	No risk
SWC-119	Shadowing State Variables	Complete	No risk
SWC-120	Weak Sources of Randomness from Chain Attributes	Complete	No risk
SWC-121	Missing Protection against Signature Replay Attacks	Complete	No risk
SWC-122	Lack of Proper Signature Verification	Complete	No risk
SWC-123	Requirement Violation	Complete	No risk
SWC-124	Write to Arbitrary Storage Location	Complete	No risk
SWC-125	Incorrect Inheritance Order	Complete	No risk
SWC-126	Insufficient Gas Griefing	Complete	No risk
SWC-127	Arbitrary Jump with Function Type Variable	Complete	No risk
SWC-128	DoS With Block Gas Limit	Complete	No risk
SWC-129	Typographical Error	Complete	No risk
SWC-130	Right-To-Left-Override control character (U+202E)	Complete	No risk
SWC-131	Presence of unused variables	Complete	No risk
SWC-132	Unexpected Ether balance	Complete	No risk

FULL AUDIT REPORT

SWC-133	Hash Collisions With Multiple Variable Length Arguments	Complete	No risk
SWC-134	Message call with hardcoded gas amount	Complete	No risk
SWC-135	Code With No Effects	Complete	No risk
SWC-136	Unencrypted Private Data On-Chain	Complete	No risk



FULL AUDIT REPORT



Visibility, Mutability, Modifier function testing

Components


 Contracts	 Libraries	 Interfaces	 Abstract
2	0	4	2

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.











 Public	 Payable			
44	1			
External	Internal	Private	Pure	View
22	45	0	1	26

StateVariables

Total	 Public
24	16



Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts	
0.8.9		yes			
 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRewriter	 New/Create/Create2
yes					



FULL AUDIT REPORT

 TryCatch	Σ Unchecked
<input type="text"/>	<input type="text" value="yes"/>



FULL AUDIT REPORT

Contracts Description Table

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
L	_msgSender	Internal 🔒		
L	_msgData	Internal 🔒		
Ownable	Implementation	Context		
L		Public !	●	NO !
L	owner	Public !		NO !
L	_checkOwner	Internal 🔒		
L	renounceOwnership	Public !	●	onlyOwner
L	transferOwnership	Public !	●	onlyOwner
L	_transferOwnership	Internal 🔒	●	
IERC20	Interface			
L	totalSupply	External !		NO !
L	balanceOf	External !		NO !
L	transfer	External !	●	NO !
L	allowance	External !		NO !
L	approve	External !	●	NO !
L	transferFrom	External !	●	NO !
IERC20Metadata	Interface	IERC20		







FULL AUDIT REPORT

Contract	Type	Bases		
L	name	External !		NO !
L	symbol	External !		NO !
L	decimals	External !		NO !
ERC20	Implementation	Context, IERC20, IERC20Metad ata		
L		Public !	●	NO !
L	name	Public !		NO !
L	symbol	Public !		NO !
L	decimals	Public !		NO !
L	totalSupply	Public !		NO !
L	balanceOf	Public !		NO !
L	transfer	Public !	●	NO !
L	allowance	Public !		NO !
L	approve	Public !	●	NO !
L	transferFrom	Public !	●	NO !
L	increaseAllowance	Public !	●	NO !
L	decreaseAllowance	Public !	●	NO !
L	_transfer	Internal 🔒	●	
L	_mint	Internal 🔒	●	
L	_burn	Internal 🔒	●	
L	_approve	Internal 🔒	●	
L	_spendAllowance	Internal 🔒	●	

FULL AUDIT REPORT



Contract	Type	Bases		
L	_beforeTokenTransfer	Internal		
L	_afterTokenTransfer	Internal		
AggregatorV3Interface	Interface			
L	decimals	External !		NO !
L	description	External !		NO !
L	version	External !		NO !
L	getRoundData	External !		NO !
L	latestRoundData	External !		NO !
IERC20USDT	Interface			
L	allowance	External !		NO !
L	transferFrom	External !		NO !
L	approve	External !		NO !
L	totalSupply	External !		NO !
L	balanceOf	External !		NO !
L	transfer	External !		NO !
AIMToken	Implementation	ERC20, Ownable		
L		Public !		ERC20
L	totalSupply	Public !		NO !
L	startTheSale	Public !		onlyOwner
L	mintByUSDT	External !		NO !

FULL AUDIT REPORT

Contract	Type	Bases		
L	mintByEth	External !		NO !
L	getLatestUSDTPrice	Public !		NO !
L	withdraw	Public !		onlyOwner
L	withdrawUSDT	Public !		onlyOwner
L	claimAIMToken	Public !		isListed
L	sellTokenInUDSTPrice	Public !		NO !
L	sellTokenInETHPrice	Public !		NO !
L	calculateTokensAmountPrice	Internal 		
L	calculateAmountInEther	Internal 		

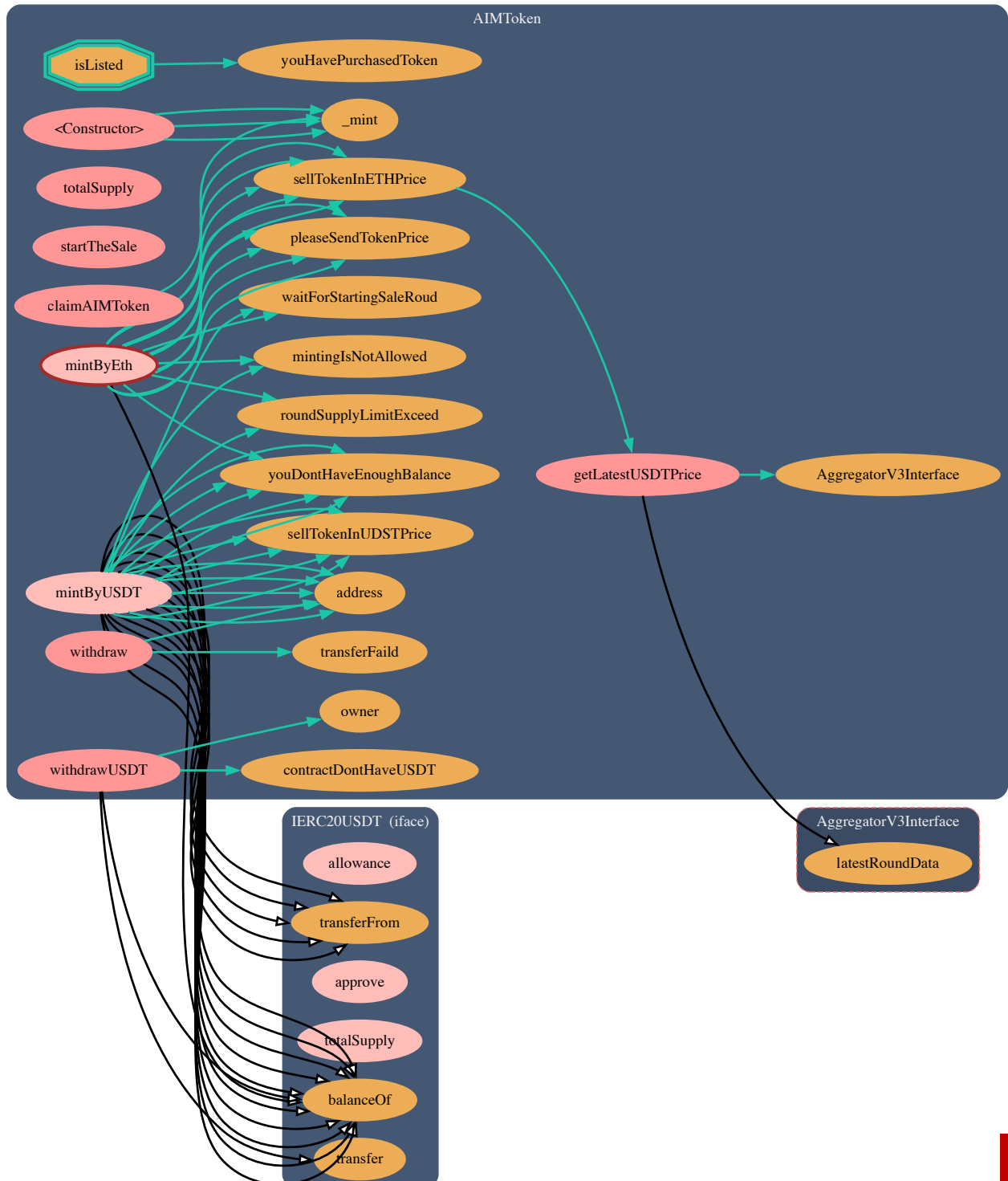
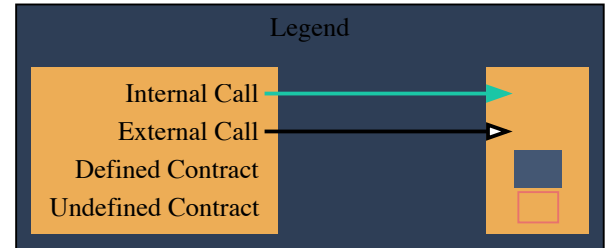


Legend

Symbol	Meaning
	Function can modify state
	Function is payable

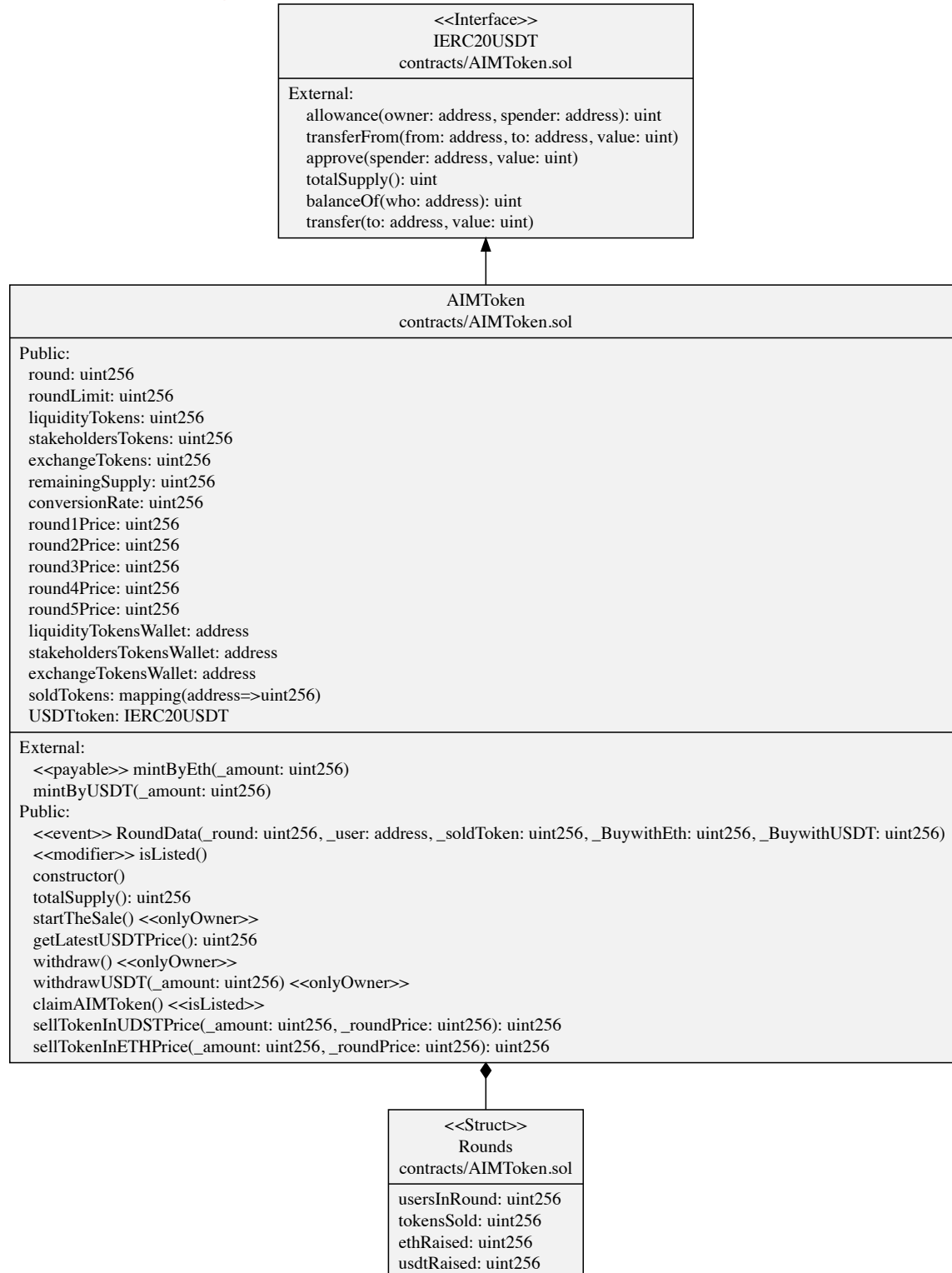
FULL AUDIT REPORT

Inheritate Function Relation Graph



FULL AUDIT REPORT

UML Class Diagram



FULL AUDIT REPORT

About SECURI LAB

SECURI LAB was established in 2020, and its goal is to deliver a security solution for Web3 projects by expert security researchers. To verify the security of smart contracts, they have developed internal tools and KYC solutions for Web3 projects using industry-standard technology. SECURI LAB was created to solve security problems for Web3 projects. They focus on technology for conciseness in security auditing. They have developed Python-based tools for their internal use called WAS and SECURI LAB. Their goal is to drive the crypto industry in Thailand to grow with security protection technology.



SECURI LAB

**Why US? — High Reliability
Intense Inspection
Affordable Price**

Cybersecurity Audit | KYC | Consultant

Follow Us On:



Website	https://securi-lab.com/
Twitter	https://twitter.com/SECURI_LAB
Telegram	https://t.me/securi_lab
Medium	https://medium.com/@securi