



# AUDIT REPORT

---

June , 2025

For



**MONWU**

# Table of Content

Executive Summary	03
Number of Security Issues per Severity	05
Summary of Issues	06
Checked Vulnerabilities	07
Techniques and Methods	09
Types of Severity	11
Severity Matrix	12
Types of Issues	13
<b>Low Severity Issues</b>	14
1. Premium Investor cannot be removed	14
2. Use ownable2step instead	15
3. Centralization Concern	16
<b>Informational Issues</b>	17
4. Emit even for critical functions	17
5. Missing functions for investors to view their claimable tokens	18
6. Unused state variable	19
7. Typo in state variable	20
Functional Tests	21
Threat Model	22
Automated Tests	29
Closing Summary & Disclaimer	29

# Executive Summary

**Project name** MONWU Smart Contract

**Protocol Type** Token

**Project URL** <https://monwu.com/>

**Overview** The MONWU protocol is a token distribution system built around an ERC20 token with a 1 billion token maximum supply. The protocol implements a sophisticated vesting mechanism where tokens are allocated across multiple investor tiers and purposes, including founders, various investor classes (Elite, Platinum, Premium), creators, community members, public sale, liquidity, rewards, marketing, and charity. Most allocations follow a 5-year vesting schedule with a 3-year cliff period followed by 2 years of gradual token releases in approximately 6-month intervals. The token includes a burn mechanism that allows holders to permanently reduce the total supply while attempting to maintain a minimum of 500 million tokens in circulation. The system is managed through six separate smart contracts - the main MONWU token contract that handles minting and burning, and five vesting contracts that manage the time-locked distribution of tokens to different participant categories. After 10 years, any unclaimed tokens can be recovered, and throughout the vesting period, contract owners maintain administrative control to add, remove, or modify investor allocations.

<b>Audit Scope</b>	The scope of this Audit was to analyze the MONWU Smart Contract Smart Contracts for quality, security, and correctness.
<b>Source Code link</b>	<a href="https://github.com/BlackH3art/monwu-token/tree/main">https://github.com/BlackH3art/monwu-token/tree/main</a>
<b>Contracts in Scope</b>	MonwuCharity.sol MonwuElite150.sol MonwuFounding15.sol MonwuMarketingDevelopment.sol MonwuPlatinum1500.sol MonwuPremiumVesting.sol TokenMonwu.sol
<b>Branch</b>	main
<b>Commit Hash</b>	547b64eb0fcfc8db3231e7b38c3dcf3deb47f002
<b>Language</b>	Solidity
<b>Blockchain</b>	EVM
<b>Method</b>	Manual Analysis, Functional Testing, Automated Testing
<b>Review 1</b>	11th June 2025 - 17th June 2025
<b>Updated Code Received</b>	19th June 2025
<b>Review 2</b>	20th June 2025
<b>Fixed In</b>	80274678b96351fe9c5d92d0fc507b22d59146ba

**Verify the Authenticity of Report on QuillAudits Leaderboard:**<https://www.quillaudits.com/leaderboard>

# Number of Issues per Severity



Critical	0 (0%)
High	0 (0%)
Medium	0 (0%)
Low	3 (43%)
Informational	4 (57%)

Issues	Severity				
	Critical	High	Medium	Low	Informational
Open	0	0	0	0	0
Acknowledged	0	0	0	1	0
Partially Resolved	0	0	0	0	0
Resolved	0	0	0	2	4

# Summary of Issues

Issue No.	Issue Title	Severity	Status
1	Premium Investor cannot be removed	Low	Resolved
2	Use ownable2step instead	Low	Resolved
3	Centralization Concern	Low	Acknowledged
4	Emit even for critical functions	Informational	Resolved
5	Missing functions for investors to view their claimable tokens	Informational	Resolved
6	Unused state variable	Informational	Resolved
7	Typo in state variable	Informational	Resolved

# Checked Vulnerabilities

<input checked="" type="checkbox"/> Access Management	<input checked="" type="checkbox"/> Compiler version not fixed
<input checked="" type="checkbox"/> Arbitrary write to storage	<input checked="" type="checkbox"/> Address hardcoded
<input checked="" type="checkbox"/> Centralization of control	<input checked="" type="checkbox"/> Divide before multiply
<input checked="" type="checkbox"/> Ether theft	<input checked="" type="checkbox"/> Integer overflow/underflow
<input checked="" type="checkbox"/> Improper or missing events	<input checked="" type="checkbox"/> ERC's conformance
<input checked="" type="checkbox"/> Logical issues and flaws	<input checked="" type="checkbox"/> Dangerous strict equalities
<input checked="" type="checkbox"/> Arithmetic Computations Correctness	<input checked="" type="checkbox"/> Tautology or contradiction
<input checked="" type="checkbox"/> Race conditions/front running	<input checked="" type="checkbox"/> Return values of low-level calls
<input checked="" type="checkbox"/> SWC Registry	<input checked="" type="checkbox"/> Missing Zero Address Validation
<input checked="" type="checkbox"/> Re-entrancy	<input checked="" type="checkbox"/> Private modifier
<input checked="" type="checkbox"/> Timestamp Dependence	<input checked="" type="checkbox"/> Revert/require functions
<input checked="" type="checkbox"/> Gas Limit and Loops	<input checked="" type="checkbox"/> Multiple Sends
<input checked="" type="checkbox"/> Exception Disorder	<input checked="" type="checkbox"/> Using suicide
<input checked="" type="checkbox"/> Gasless Send	<input checked="" type="checkbox"/> Using delegatecall
<input checked="" type="checkbox"/> Use of tx.origin	<input checked="" type="checkbox"/> Upgradeable safety
<input checked="" type="checkbox"/> Malicious libraries	<input checked="" type="checkbox"/> Using throw

Using inline assembly

Unsafe type inference

Style guide violation

Implicit visibility level

# Techniques and Methods

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

- The overall quality of code.
- Use of best practices.
- Code documentation and comments, match logic and expected behavior.
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Implementation of ERC 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 analyzed 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

A 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 analyzed, 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 behavior 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, Foundry, Solhint, Mythril, Slither, Solidity Static Analysis.

# Types of Severity

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

## **Critical: Immediate and Catastrophic Impact**

Critical issues are the ones that an attacker could exploit with relative ease, potentially leading to an immediate and complete loss of user funds, a total takeover of the protocol's functionality, or other catastrophic failures. Critical vulnerabilities are non-negotiable; they absolutely must be fixed.

## **High (H): Significant Risk of Major Loss or Compromise**

High-severity issues represent serious weaknesses that could result in significant financial losses for users, major malfunctions within the protocol, or substantial compromise of its intended operations. While exploiting these vulnerabilities might require specific conditions to be met or a moderate level of technical skill, the potential damage is considerable. These findings are critical and should be addressed and resolved thoroughly before the contract is put into the Mainnet.

## **Medium (M): Potential for Moderate Harm Under Specific Circumstances**

Medium-severity bugs are loopholes in the protocol that could lead to moderate financial losses or partial disruptions of the protocol's intended behavior. However, exploiting these vulnerabilities typically requires more specific and less common conditions to occur, and the overall impact is generally lower compared to high or critical issues. While not as immediately threatening, it's still highly recommended to address these findings to enhance the contract's robustness and prevent potential problems down the line.

## **Low (L): Minor Imperfections with Limited Repercussions**

Low-severity issues are essentially minor imperfections in the smart contract that have a limited impact on user funds or the core functionality of the protocol. Exploiting these would usually require very specific and unlikely scenarios and would yield minimal gain for an attacker. While these findings don't pose an immediate threat, addressing them when feasible can contribute to a more polished and well-maintained codebase.

## **Informational (I): Opportunities for Improvement, Not Immediate Risks**

Informational findings aren't security vulnerabilities in the traditional sense. Instead, they highlight areas related to the clarity and efficiency of the code, gas optimization, the quality of documentation, or adherence to best development practices. These findings don't represent any immediate risk to the security or functionality of the contract but offer valuable insights for improving its overall quality and maintainability. Addressing these is optional but often beneficial for long-term health and clarity.

# Severity Matrix

		Impact		
		High	Medium	Low
Likelihood	High	Critical	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

## Impact

- **High** - leads to a significant material loss of assets in the protocol or significantly harms a group of users.
- **Medium** - only a small amount of funds can be lost (such as leakage of value) or a core functionality of the protocol is affected.
- **Low** - can lead to any kind of unexpected behavior with some of the protocol's functionalities that's not so critical.

## Likelihood

- High - attack path is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount of funds that can be stolen or lost.
- Medium - only a conditionally incentivized attack vector, but still relatively likely.
- Low - has too many or too unlikely assumptions or requires a significant stake by the attacker with little or no incentive.

# Types of Issues

<b>Open</b>  Security vulnerabilities identified that must be resolved and are currently unresolved.	<b>Resolved</b>  Security vulnerabilities identified that must be resolved and are currently unresolved.
<b>Acknowledged</b>  Vulnerabilities which have been acknowledged but are yet to be resolved.	<b>Partially Resolved</b>  Considerable efforts have been invested to reduce the risk/ impact of the security issue, but are not completely resolved.

# Low Severity Issues

## Premium Investor cannot be removed

Resolved

### Path

MONWUPremiumVesting.sol

### Description

MONWUPremiumVesting contract lacks remove and edit functions that exist in all other vesting contracts. Once added, premium investors cannot be removed or have their allocations adjusted, even if added by mistake.

### Recommendation

Consider adding a functionality to remove premium investors

**Use ownable2step instead****Resolved****Description**

Contracts use basic Ownable which allows single-step ownership transfer. Should use Ownable2Step to prevent accidental transfer to wrong address. Current implementation could permanently lock owner functions if transferred to incorrect address.

**Recommendation**

Consider using Ownable2Step.sol instead.

## Centralization Concern

Acknowledged

### Description

The current implementation of contract poses centralization risk where a single owner address has complete control over investor allocations, can remove investors, edit allocations after vesting starts, and claim all leftover tokens. No multi-sig or time-lock mechanisms.

The contract has a wide attack surface provided that the owner address is compromised.

### Recommendation

Ensure that the owner is a multisig wallet

# Informational Severity Issues

## Emit even for critical functions

Resolved

### Path

-

### Function

handleLeftovers()

### Description

handleLeftovers() transfers potentially large amounts of tokens but emits no event. Makes it difficult to track 10-year token movements on-chain. Should emit an event with the recipient and amount.

### Recommendation

Consider adding an event for this function.

## Missing functions for investors to view their claimable tokens

Resolved

### **Path**

-

### **Function**

-

### **Description**

There is no public view function like getReleasableAmount() for investors to check available tokens before attempting withdrawal.

As a result, users must waste gas on failed withdrawal attempts to discover the available amount.

## Unused state variable

Resolved

### Path

MONWU.sol

### Function

burn()

### Description

The burned state variable is incremented but never read or used in any logic. The burn protection check uses `cap` instead.

### Recommendation

Either use the variable for protection logic or remove it to save gas.

## Typo in state variable

Resolved

### Path

-

### Function

-

### Description

Inconsistent naming: elit150Initialized missing 'e' (should be elite150Initialized).

### Recommendation

Consider fixing the typo

# Functional Tests

**Some of the tests performed are mentioned below:**

- ✓ Should revert when burn would reduce cap below 500M
- ✓ Should include vested but unclaimed tokens in handleLeftovers after 10 years
- ✓ Should create vesting schedule with 3-year cliff
- ✓ Should release 100% of allocation after vesting end
- ✓ Should transfer remaining tokens via handleLeftovers

# Threat Model

Contract	Function	Threats
Vesting Contract	addInvestor() / addEliteInvestor() / addFounder() / addPlatinumInvestor() / addPremiumInvestor()	<p><b>Inputs</b></p> <ul style="list-style-type: none"> <li>investor (address) - The investor address to add           <ul style="list-style-type: none"> <li>Control: Fully controlled by owner</li> <li>Constraints: Must not already exist in mapping</li> <li>Impact: Determines who can claim tokens</li> </ul> </li> <li>allocation (uint256) - Token amount to allocate           <ul style="list-style-type: none"> <li>Control: Fully controlled by owner</li> <li>Constraints: None (can be 0 or any value)</li> <li>Impact: Determines vesting amount</li> </ul> </li> </ul> <p><b>Internal State Dependencies</b></p> <ul style="list-style-type: none"> <li>addressToInvestor[investor]</li> <li>Control: Modified by add/remove/edit functions</li> <li>Constraints: investor field must be address(0) to add</li> <li>Impact: Stores vesting schedule and allocation</li> <li>block.timestamp</li> <li>Control: None (external dependency)</li> <li>Constraints: None</li> <li>Impact: Determines token precision</li> <li>MONWUToken.decimals()</li> </ul>

Contract	Function	Threats
	<pre>removeInvestor() / removeEliteInvestor() / removeFounder() / removePlatinumInvestor() ()</pre>	<ul style="list-style-type: none"> <li>• Control: None (external dependency)</li> <li>• Constraints: None</li> <li>• Impact: Determines token precision</li> </ul> <p><b>Branches and Code Coverage</b></p> <p>Intended branches</p> <ul style="list-style-type: none"> <li>• Should add new investor with allocation</li> <li>• Should calculate cliff end (3 years from now)</li> <li>• Should calculate vesting end (5 years from now)</li> <li>• Should emit InvestorAdded event</li> <li>• Should scale allocation by token decimals</li> </ul> <p><b>Negative behavior</b></p> <ul style="list-style-type: none"> <li>• Should not allow adding existing investor</li> <li>• Currently allows address(0) as investor (critical bug)</li> </ul> <p>Currently allows 0 allocation (gas waste)</p> <ul style="list-style-type: none"> <li>• No maximum allocation check</li> <li>• Only callable by owner (centralization)</li> <li>• For Premium: requires token transfer approval</li> </ul> <p><b>Inputs</b></p> <ul style="list-style-type: none"> <li>• investor (address) - The investor to remove <ul style="list-style-type: none"> <li>• Control: Fully controlled by owner</li> <li>• Constraints: Must exist in mapping</li> </ul> </li> </ul> <p>Impact: Removes access to tokens</p>

Contract	Function	Threats
	<pre>editInvestor() / editEliteInvestor() / editFounder() / editPlatinumInvestor()</pre>	<p><b>Internal State Dependencies</b></p> <ul style="list-style-type: none"> <li>• addressToInvestor[investor] <ul style="list-style-type: none"> <li>• Control: Modified by this function</li> <li>• Constraints: investor field must not be address(0)</li> <li>• Impact: Zeros address and allocation only</li> </ul> </li> </ul> <p><b>Branches and Code Coverage</b></p> <p><b>Intended branches</b></p> <ul style="list-style-type: none"> <li>• Should remove investor access</li> <li>• Should emit InvestorRemoved event</li> </ul> <p><b>Negative behavior</b></p> <ul style="list-style-type: none"> <li>• Missing from MONWUPremiumVesting <ul style="list-style-type: none"> <li>• (inconsistency bug) Doesn't clear all struct fields</li> <li>• (gas inefficiency) Tokens remain locked in</li> </ul> </li> <li>• contract (design flaw) <ul style="list-style-type: none"> <li>• Can remove after partial</li> </ul> </li> <li>• withdrawal (accounting issue) <ul style="list-style-type: none"> <li>• Only callable by owner (centralization)</li> </ul> </li> </ul> <p><b>Inputs</b></p> <ul style="list-style-type: none"> <li>• investor (address) - The investor to edit <ul style="list-style-type: none"> <li>• Control: Fully controlled by owner</li> <li>• Constraints: Must exist in mapping</li> <li>• Impact: Identifies which allocation to modify</li> </ul> </li> </ul>

Contract	Function	Threats
		<ul style="list-style-type: none"> <li>newAllocation (uint256) - New token amount</li> <li>Control: Fully controlled by owner</li> <li>Constraints: None</li> <li>Impact: Changes vesting amount</li> </ul> <p><b>Internal State Dependencies</b></p> <ul style="list-style-type: none"> <li>addressToInvestor[investor].allocation</li> <li>Control: Modified by this function</li> <li>Constraints: None</li> <li>Impact: Changes total claimable amount</li> </ul> <p><b>Branches and Code Coverage</b></p> <p><b>Intended branches</b></p> <p>Should update allocation Should emit InvestorEdited event</p> <p><b>Negative behavior</b></p> <ul style="list-style-type: none"> <li>Missing from MONWUPremiumVesting (inconsistency bug)</li> <li>Can set allocation below already withdrawn amount (critical bug)</li> <li>No recalculation of vesting schedule (logic bug)</li> <li>Allows retroactive vesting if allocation increased (exploit)</li> <li>Only callable by owner (centralization)</li> </ul>

Contract	Function	Threats
	<code>investorRelease()</code> / <code>founderRelease()</code>	<p><b>Inputs</b></p> <ul style="list-style-type: none"> <li>• amount (uint256) - Amount to withdraw</li> <li>• Control: Fully controlled by caller</li> <li>• Constraints: Must not exceed releasable</li> <li>• amount Impact: Determines tokens transferred</li> </ul> <p><b>Internal State Dependencies</b></p> <ul style="list-style-type: none"> <li>• <code>addressToInvestor[msg.sender]</code></li> <li>• Control: Released field modified by this function</li> <li>• Constraints: Must be valid investor</li> <li>• Impact: Tracks withdrawal progress</li> <li>• <code>block.timestamp</code> <ul style="list-style-type: none"> <li>• Control: None (blockchain controlled)</li> <li>• Constraints: Must be past cliff end</li> <li>• Impact: Determines releasable amount</li> </ul> </li> <li>• <code>MONWUToken.balanceOf(address(this))</code></li> <li>• Control: None (depends on token balance)</li> <li>• Constraints: Must have sufficient balance</li> <li>• Impact: Limits withdrawal capability</li> </ul>

Contract	Function	Threats
	handleLeftovers()	<p><b>Branches and Code Coverage</b></p> <ul style="list-style-type: none"> <li>• Intended branches           <ul style="list-style-type: none"> <li>• Should calculate correct releasable amount</li> <li>• Should transfer tokens to investor</li> <li>• Should update released amount</li> <li>• Should emit ReleaseTokens event</li> <li>• Should handle precision loss at vesting end</li> </ul> </li> </ul> <p><b>Negative behavior</b></p> <ul style="list-style-type: none"> <li>• Integer division causes precision loss (minor bug)</li> <li>• Misleading vesting schedule (4 periods + remainder)</li> <li>• No view function to check releasable amount</li> <li>• Can't withdraw during cliff period</li> </ul> <p><b>Inputs</b></p> <ul style="list-style-type: none"> <li>• No external inputs</li> </ul> <p><b>Internal State Dependencies</b></p> <ul style="list-style-type: none"> <li>• block.timestamp           <ul style="list-style-type: none"> <li>• Control: None (blockchain controlled)</li> <li>• Constraints: Must be &gt; burnDeadline (10 years)</li> <li>• Impact: Enables function execution</li> </ul> </li> </ul>

Contract	Function	Threats
		<ul style="list-style-type: none"> <li>• MONWUToken.balanceOf(address(this))</li> <li>• Control: None</li> <li>• Constraints: Must be &gt; 0</li> <li>• Impact: Determines transfer amount</li> <li>• MONWUToken.owner()</li> <li>• Control: None (external dependency)</li> <li>• Constraints: None</li> <li>• Impact: Determines recipient (bug - wrong recipient)</li> </ul> <p><b>Branches and Code Coverage</b></p> <p><b>Intended branches</b></p> <ul style="list-style-type: none"> <li>• Should transfer remaining tokens after 10 years</li> <li>• Should only work after deadline</li> </ul> <p><b>Negative behavior</b></p> <ul style="list-style-type: none"> <li>• Sends to token owner, not contract owner (critical bug)</li> <li>• Takes legitimate vested tokens too (design flaw)</li> <li>• No event emitted (transparency issue)</li> <li>• Only callable by owner (expected)</li> </ul>

# Automated Tests

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

# Closing Summary

In this report, we have considered the security of MONWU Smart Contract. We performed our audit according to the procedure described above.

Issues of Low and Informational severity were found. The MONWU team acknowledged one finding and successfully resolved all remaining issues.

# Disclaimer

At QuillAudits, we have spent years helping projects strengthen their smart contract security. However, security is not a one-time event—threats evolve, and so do attack vectors. Our audit provides a security assessment based on the best industry practices at the time of review, identifying known vulnerabilities in the received smart contract source code.

This report does not serve as a security guarantee, investment advice, or an endorsement of any platform. It reflects our findings based on the provided code at the time of analysis and may no longer be relevant after any modifications. The presence of an audit does not imply that the contract is free of vulnerabilities or fully secure.

While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

Stay proactive. Stay secure.



# About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem



<b>7+</b> Years of Expertise	<b>1M+</b> Lines of Code Audited
<b>\$30B+</b> Secured in Digital Assets	<b>1400+</b> Projects Secured

Follow Our Journey



# AUDIT REPORT

---

June , 2025

For



MONWU



Canada, India, Singapore, UAE, UK

[www.quillaudits.com](http://www.quillaudits.com)    [audits@quillaudits.com](mailto:audits@quillaudits.com)