



CHAINPROOF

# Audit Report

## Fin AI

May 2025

Network BSC

Address 0x884113738e307265ff84e2a0f5f2f98f01854543

Audited by © ChainProof

# Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed



# Table of Contents

<b>Analysis</b>	1
<b>Table of Contents</b>	2
<b>Risk Classification</b>	3
<b>Review</b>	3
Audit Updates	4
Source Files	4
<b>Findings Breakdown</b>	5
<b>Functions Analysis</b>	6
<b>Inheritance Graph</b>	7
<b>Flow Graph</b>	8
<b>Summary</b>	8
<b>Disclaimer</b>	9
<b>About Chainproof</b>	<b>12</b>



## Risk Classification

The criticality of findings in Chainproof's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation:** This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation:** This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical:** Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium:** Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor:** Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative:** Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact
● Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
● Minor / Informative	Unlikely / Low to no Impact

## Review

Contract Name	Redis
---------------	-------



Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Explorer	<a href="https://bscscan.com/address/0x884113738e307265ff84e2a0f5f2f98f01854543">https://bscscan.com/address/0x884113738e307265ff84e2a0f5f2f98f01854543</a>
Address	0x884113738e307265ff84e2a0f5f2f98f01854543
Network	BSC
Symbol	FIN
Decimals	18
Total Supply	1.000.000.000
Badge Eligibility	Yes

## Audit Updates

Initial Audit	13 May 2025 <a href="https://github.com/Chainproof-io/audits/blob/main/6-fin/v1/audit.pdf">https://github.com/Chainproof-io/audits/blob/main/6-fin/v1/audit.pdf</a>
Corrected Phase 2	16 May 2025




## Source Files

Filename	SHA256
----------	--------

**Redis.sol**

c68d6c9f85a39921e395102c685d0dc67e49da450f43244cf7e86f361c153ef9

## Findings Breakdown

Severity	Unresolved	Acknowledged	Resolved	Other
 Critical	0	0	0	0
 Medium	0	0	0	0
 Minor / Informative	0	0	0	0

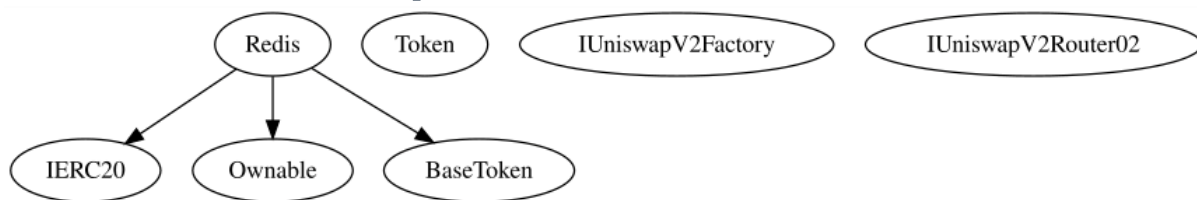
# Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Redis	Implementation	IERC20, Ownable, BaseToken		
		Public	Payable	-
	getNativeCurrency	Internal		
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	tokenFromReflection	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokensForEth	Private	✓	lockTheSwap
	withdrawETH	External	✓	onlyOwner



	withdrawTokens	External	✓	onlyOwner
	setTreasuryAddress	External	✓	onlyOwner
	_transferStandard	Private	✓	
		External	Payable	-
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	manualSwap	External	✓	onlyOwner
	setFee	Public	✓	onlyOwner
	validateFees	Internal		
	toggleSwap	External	✓	onlyOwner
	excludeMultipleAccountsFromFees	External	✓	onlyOwner
	getExcludedFromFee	External		-

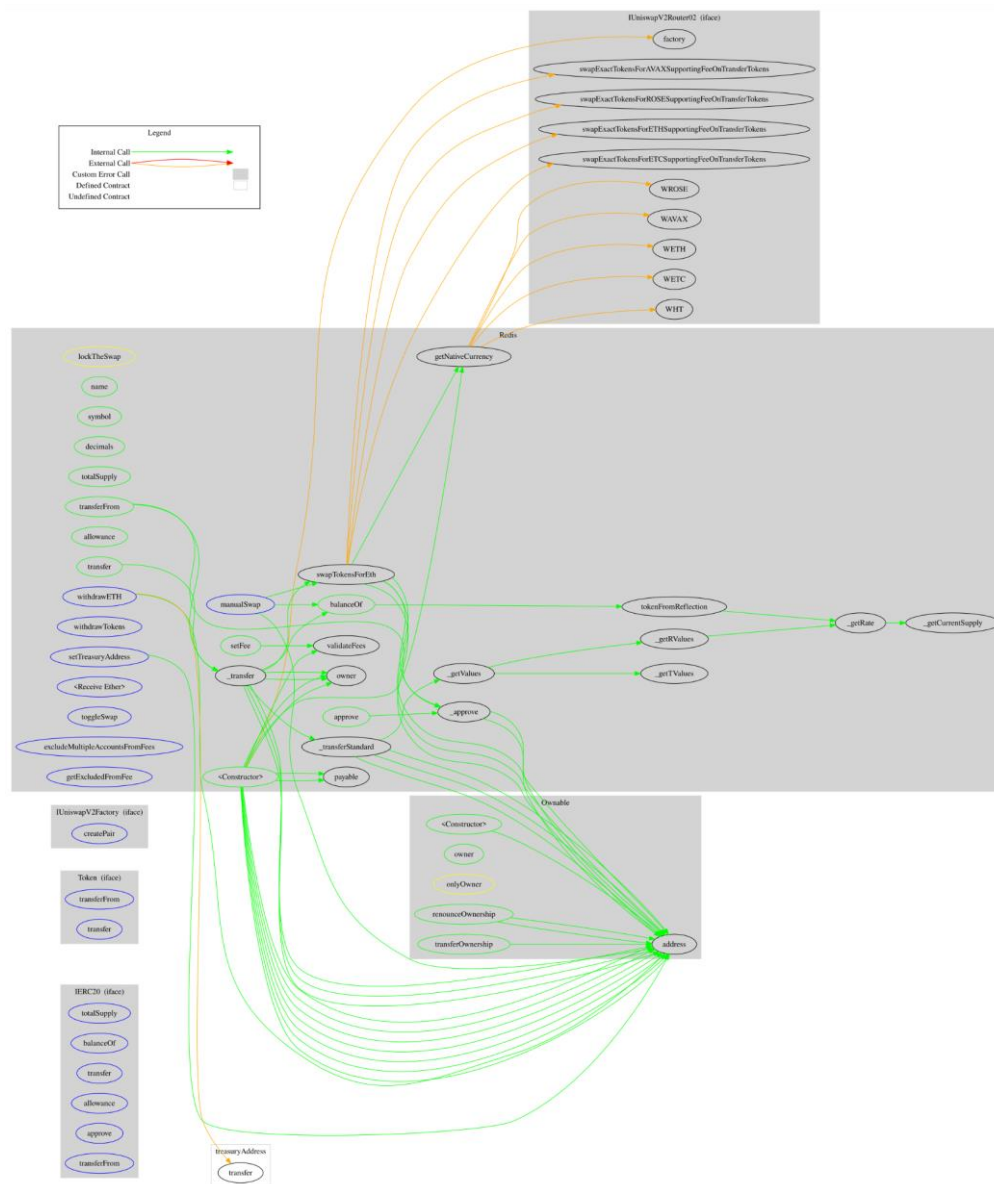
## Inheritance Graph







# Flow Graph



## Summary

Fin AI contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Fin AI is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 20% fees.



## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Chainproof's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Chainproof to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Chainproof's position is that each company and individual are responsible for their own due diligence and continuous security. Chainproof's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Chainproof are subject to dependencies and are under continuing development. 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. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

# About ChainProof

Chainproof is an Audit & KYC firm for Blockchain Projects, aimed at securing the Blockchain and the assets at risk. Chainproof is fueled by Industry grade experienced Blockchain Developers from all around the globe. From finding vulnerabilities, potential scams, malicious code mitigation, improper implementation of the token which can lead to loss of user's fund, you name it and we cover and secure them all.

Security testing and risk mitigation is given the highest priority at ChainProof. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

ChainProof is aiming to make crypto discoverable and efficient globally. We associate with extremely robust testing and code review, leaving no room for any security risks because, when it comes to user's funds, we need to leave no stone unturned. Cheers!



# CHAINPROOF

**The ChainProof team**

ChainProof.dev