freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

HyprBurnTier

03/09/2025

TOKEN OVERVIEW

Fees

- Buy fees: N/A
- Sell fees: N/A

Fees privileges

- Not available

Ownership

- Owned

Minting

- Mint function not detected

Max Tx Amount / Max Wallet Amount

- Not available

Blacklist

- Blacklist function not detected

Other privileges

- Not available

TABLE OF CONTENTS

1 DISCLAIMER

2 INTRODUCTION

3 WEBSITE + SOCIALS

4-5 AUDIT OVERVIEW

6-8 OWNER PRIVILEGES & FINDINGS

9 CONCLUSION AND ANALYSIS

10 TOKEN DETAILS

11 HYPR TOKEN ANALYTICS &
TOP 10 TOKEN HOLDERS

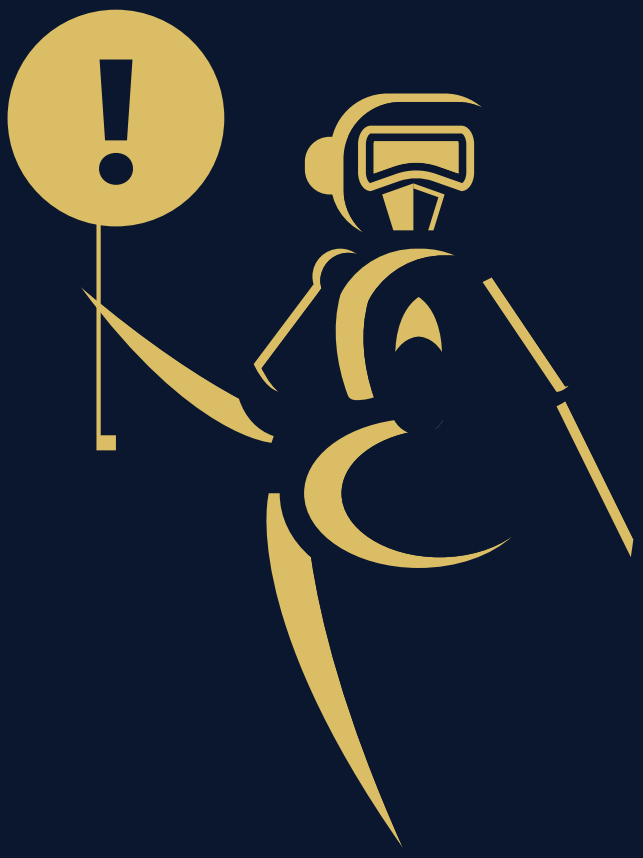
12 TECHNICAL DISCLAIMER

DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website https://freshcoins.io
FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by HYPR (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0xf1cdCB6A7f97AFfc0C5CFe4b7D5Ba6d5376201ca

Network: Ethereum (ETH)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 03/09/2025

WEBSITE DIAGNOSTIC

https://hypr.fund/

0-49 50-89 90-100

Performance | Accessibility | Best Practices | SEO | Progressive Web App

Socials

X (Twitter)

https://x.com/hyprfund

Telegram

https://t.me/hyprfund

AUDIT OVERVIEW

94

Security Score

95

Static Scan
Automatic scanning for common vulnerabilities

93

ERC Scan
Automatic checks for ERC's conformance

0 High

0 Medium

0 Low

2 Optimizations

0 Informational

No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Low
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES & FINDINGS

Centralization Risk Due to Owner Privileges

The owner can arbitrarily change Supr and Hypr thresholds, potentially devaluing prior burns or altering tier progression. No timelock or multi-signature protection exists, so a compromised or malicious owner could affect users' burn-based tiers.

Consider adding a timelock for critical owner functions or migrating to a DAO/multi-sig ownership post-deployment. Renounce ownership if no further changes are needed. This is a general best practice for production contracts.

No Bulk Burn Functionality

Users can only burn in single transactions via burn or burnWithPermit. For large or multiple burns, this increases gas costs and user friction, though it's not a security issue.

Add a burnBatch function accepting an array of amounts if frequent bulk operations are expected. This is an optimization suggestion.

Workflow

The HyprBurnTier contract lets users burn an ERC-20 token to reach higher tier statuses (Commonr → Supr → Hypr) based on cumulative burned amounts. A user first approves the contract to spend their tokens (or later, potentially uses permit), then calls burn(amount) to destroy tokens for themselves or burnFor(amount, destination) to credit another address; under the hood, tokens are transferred from the user to the dead address, the burn is recorded, and the credited account's tier is updated if thresholds are crossed. The contract tracks per-wallet burned totals and tiers, allows the owner to adjust tier thresholds (either in raw smallest units or in whole tokens based on decimals), and exposes views so anyone can check an account's tier, thresholds, or total tokens burned. Events are emitted on burns, threshold updates, and tier changes, providing a transparent workflow where burning increases recognition tier while ensuring tokens are irreversibly destroyed.

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.

CONCLUSION AND ANALYSIS

Smart Contracts within the scope were manually reviewed and analyzed with static tools.

Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.

Found no HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	N/A
Sell fees:	N/A
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	Owned
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

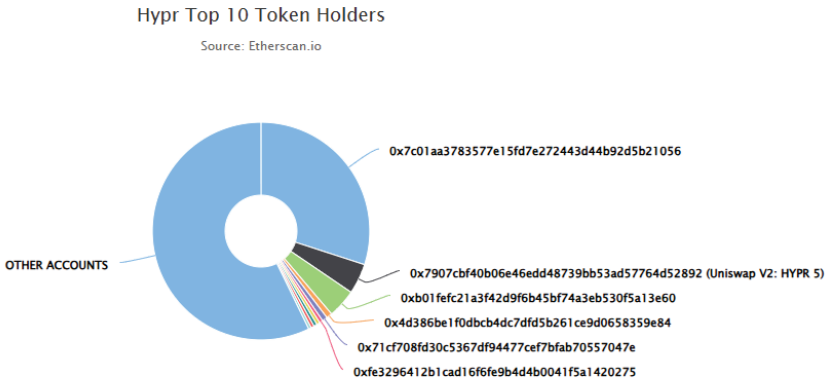
Rug Pull Risk

Liquidity:	N/A
Holders:	Clean

HYPR TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

The top 10 holders collectively own 42.79% (427,940,055.37 Tokens) of Hypr

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 1,906



(A total of 427,940,055.37 tokens held by the top 10 accounts from the total supply of 1,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x7C01AA37...2d5b21056	300,000,000	30.0000%
2	Uniswap V2: HYPR 5	45,077,774.460574132	4.5078%
3	0xb01fEFC2...0f5a13E60	42,698,990.33	4.2699%
4	0x4D386bE1...658359e84	8,579,543.444998304	0.8580%
5	0x71Cf708f...70557047E	7,900,000	0.7900%
6	0xfe329641...5A1420275	5,000,000	0.5000%
7	0xFFF03526...719b8cfe2	5,000,000	0.5000%
8	0x7d56675a...Ac916D8BF	5,000,000	0.5000%
9	0x52CDd240...3F5AeB44B	4,573,000	0.4573%
10	0xEAEE61b8...603F47AcF	4,110,747.13382203	0.4111%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.