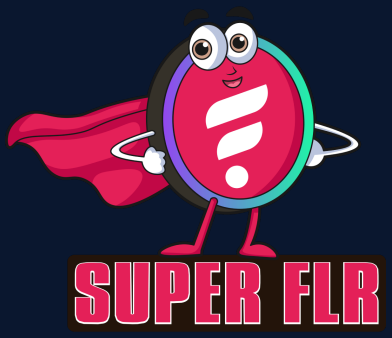
freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



SuperFlare

$SUPERFLR

29/04/2024

TOKEN OVERVIEW

Fees

- Buy fees: 2% burn
- Sell fees: 2% burn

Fees privileges

- Can’t set or change fees

Ownership

- Ownership renounced

Minting

- No mint function

Max Tx Amount / Max Wallet Amount

- Can’t change max tx amount and / or max wallet amount

Blacklist

- Blacklist function not detected

Other privileges

- N/A

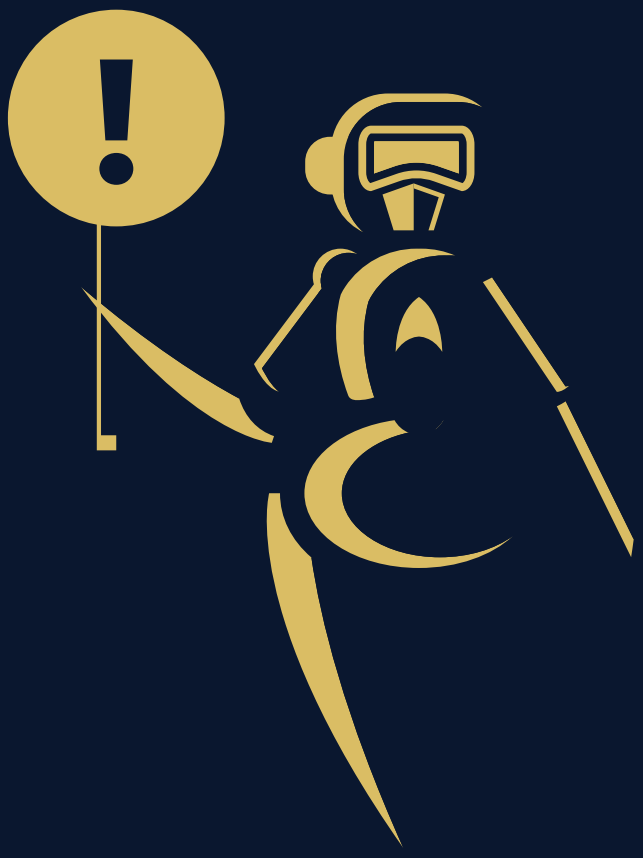
TABLE OF CONTENTS

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 SuperFlare (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0x5701113457375f8e78e46238533a27ba3e375d76

Network: Flare Network (FLARE)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 29/04/2024

WEBSITE DIAGNOSTIC

https://superflare.fun/


0-49


50-89


90-100

Performance

Accessibility

Best Practices

SEO

Progressive Web App

Socials


Twitter

https://twitter.com/SuperFlareCoin


Telegram

https://t.me/SuperFlarecoin

AUDIT OVERVIEW

91

Security Score

98

Static Scan
Automatic scanning for common vulnerabilities

90

ERC Scan
Automatic checks for ERC's conformance

0 High

0 Medium

0 Low

0 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	Low
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

Ownership renounced

Transaction Details

Transaction Hash	0xf4a0665083650a66e781c0b9376e88ac5e6f2a15baeb7cdddc31369f464e90c7
Result	Success
Status	Confirmed — Confirmed by 418,076
Block	22797021
Timestamp	9 days ago | April-20-2024 07:42:15 PM +3 UTC | Confirmed within <= 1.939 seconds
From	0xc3bF26633EbAD2FEf955Bd0febAf6E2f347Bf777
Interacted With (To)	SuperFlare (0x570111-375d76)
Value	0 FLR
Transaction Fee	0.0007722825 FLR
Gas Price	27.5 Gwei
Transaction Type	2 (EIP-1559)
Gas Limit	28,083
Max Fee per Gas	54.59853 Gwei
Max Priority Fee per Gas	2.5 Gwei
Priority Fee / Tip	0.0000702075 FLR
Transaction Burnt Fee	0.000702075 FLR
Gas Used by Transaction	28,083 | 100%
Nonce Position	242 1
Raw Input	Hex (Default)

```
0x71501886
```

Input

Method Id	0x715018a6
Call	renounceOwnership()

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:	2% burn
Sell fees:	2% burn
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

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

Others

Liquidity:	0x30b6254dd20e557380b237a7d58119710494d451
Holders:	Clean

SUPERFLR TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

Token Holders

Page 1

BlazeSwap (0x30b625...94d451)
22,845,441,814.636 SUPERFLR 30.3633%

0xc3bF26633EbAD2FEf955Bd0febAf6E2f347Bf777
19,261,574,839.99 SUPERFLR 25.6001%

0x822994de93544Ed876FF87f953bf7D030dFC746b
10,000,000,000 SUPERFLR 13.2907%

0x943E22d186dBBd9A023d508b90D8F7DAE57d27e7
2,800,000,000 SUPERFLR 3.7214%

0x53A633a02A8282eD464Fc5d7F09D30CB05cF2FBf
2,073,216,693.693 SUPERFLR 2.7555%

0x008220220fb2797bc5439dFd938679B224943C55
1,917,328,618.427 SUPERFLR 2.5483%

0x09604c9E09c6238eF9F451554fa5B140c3cEd460
1,750,000,000 SUPERFLR 2.3259%

0xE13d99b7C8feb201abdD08bc141ee9d3e3C45e39
1,127,112,957.684 SUPERFLR 1.4980%

0xC8Bb23c2f387543ec86eC72b39206fB46C623760
990,224,815.542 SUPERFLR 1.3161%

0x2c189C336129c0a89f95AC6C57DCC9C726cc31e7
921,418,226.412 SUPERFLR 1.2246%

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.