SPYWOLF

Security Audit Report
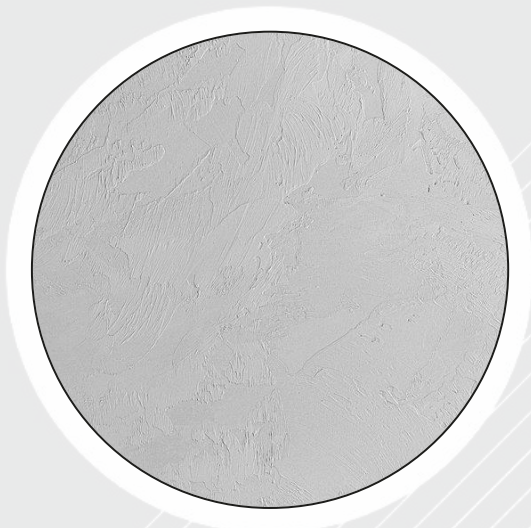
Audit prepared for

LightChainAI

Completed on

November 28, 2024

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> – SPYWOLF Team –

TABLE OF CONTENTS

LightChainAI

PROJECT DESCRIPTION:

No information yet

Release Date: TBD

Launchpad: TBD

Category: Token

01

KEY RESULTS

Cannot mint new tokens	PASSED
Cannot pause trading (honeypot)	PASSED
Cannot blacklist an address	PASSED
Cannot raise taxes over 25%?	PASSED
No proxy contract detected	PASSED
Not required to enable trading	NOT PASSED
No hidden ownership	PASSED
Cannot change the router	PASSED
No cooldown feature found	PASSED
Bot protection delay is lower than 5 blocks	PASSED
Cannot set max tx amount below 0.05% of total supply	PASSED
The contract cannot be self-destructed by owner	PASSED

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

CONTRACT INFO

Token Name
LightChainAI

Symbol
LCAI

Contract Address
0x9cA8530CA349c966Fe9ef903Df17a75B8A778927

Network
ETH

Language
Solidity

Deployment Date
Nov 25, 2024

Contract Type
Standard token

Total Supply
10,000,000,000

Decimals
18

TAXES

Buy Tax
0%

Sell Tax
0%

*Taxes cannot be changed

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

SPYWOLF.CO

SMART CONTRACT STATS

Calls Count	55
External calls	5
Internal calls	50
Transactions count	52
Last transaction time	2024-11-28 08:01:23 UTC
Deployment Date	2024-11-25 09:57:47 UTC
Create TX	0x3b6d28b908636a3c3678462794232a8466a5b4836e199716150e102c0a7a3ae4
Owner	0xfbE810101064E326f871bf20576d8e42C75d5Dd7
Deployer	0xfbE810101064E326f871bf20576d8e42C75d5Dd7

TOKEN TRANSFERS STATS

Transfer Count	48
Total Amount	22003414621.470287 LCAI
Median Transfer Amount	35714.28571428571 LCAI
Average Transfer Amount	458404471.28063095 LCAI
First transfer date	2024-11-25
Last transfer date	2024-11-28
Days token transferred	4 Days

03

FEATURED WALLETS

Owner address	0xfbE810101064E326f871bf20576d8e42C75d5Dd7
Marketing fee receiver	Unavailable
LP address	**Uniswap:** Liquidity is not added yet

TOP 3 UNLOCKED WALLETS

59.99%	Same as owner 0xfbE810101064E326f871bf20576d8e42C75d5Dd7
39.96%	Presale contract 0x7f5620c13b1644b4244114B465fA71Bd95F1d8Dc
Unavailable	

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Reentrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

05-A

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

05-B

VULNERABILITY ANALYSIS
NO ERRORS FOUND

MANUAL
CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

07

FOUND THREATS

⚠️ High Risk: 0

No high risk-level threats found in this contract.

⚠️ Medium Risk: 0

No medium risk-level threats found in this contract.

⚠️ Low Risk: 0

No low risk-level threats found in this contract.

08-A

FOUND THREATS

ℹ️ Informational: 2

Owner can enable trading once (set 'trading' state variable to true).
Once enabled, trading cannot be disabled.
Trading is currently disabled.

```solidity
function enableTrading() external onlyOwner {
    require(!trading, "LightchainAI: Trading is already enabled");
    trading = true;
}
```

Note:
Trading will still be possible when trading is disabled ('trading' state var is false), if the liquidity pool is added to whitelist. For trading to be enabled permanently, 'trading' state variable must be set to true.

Owner can white list address.
Whitelisted addresses can transfer tokens, before the trading is enabled.

```solidity
function setWhitelist(address _user, bool _status) external onlyOwner {
    whitelist[_user] = _status;
    emit WhitelistUpdated(_user, _status);
}

function _transfer(address from, address to, uint256 amount) private {
    require(from != address(0), "LightchainAI: Transfer from zero address");
    require(to != address(0), "LightchainAI: Transfer to zero address");
    require(amount > 0, "LightchainAI: Transfer amount must be greater than zero");

    if (!whitelist[from] && !whitelist[to]) {
        require(trading, "LightchainAI: Trading is disabled");
    }
    ......................
}
```

08-B

The following tokenomics are based on Etherscan:

Tokenomics:

Deployer - 60%,

Presale contract - 40%,

Token Distribution

Tokens distribution

Presale
40,0%

Deployer
60,0%
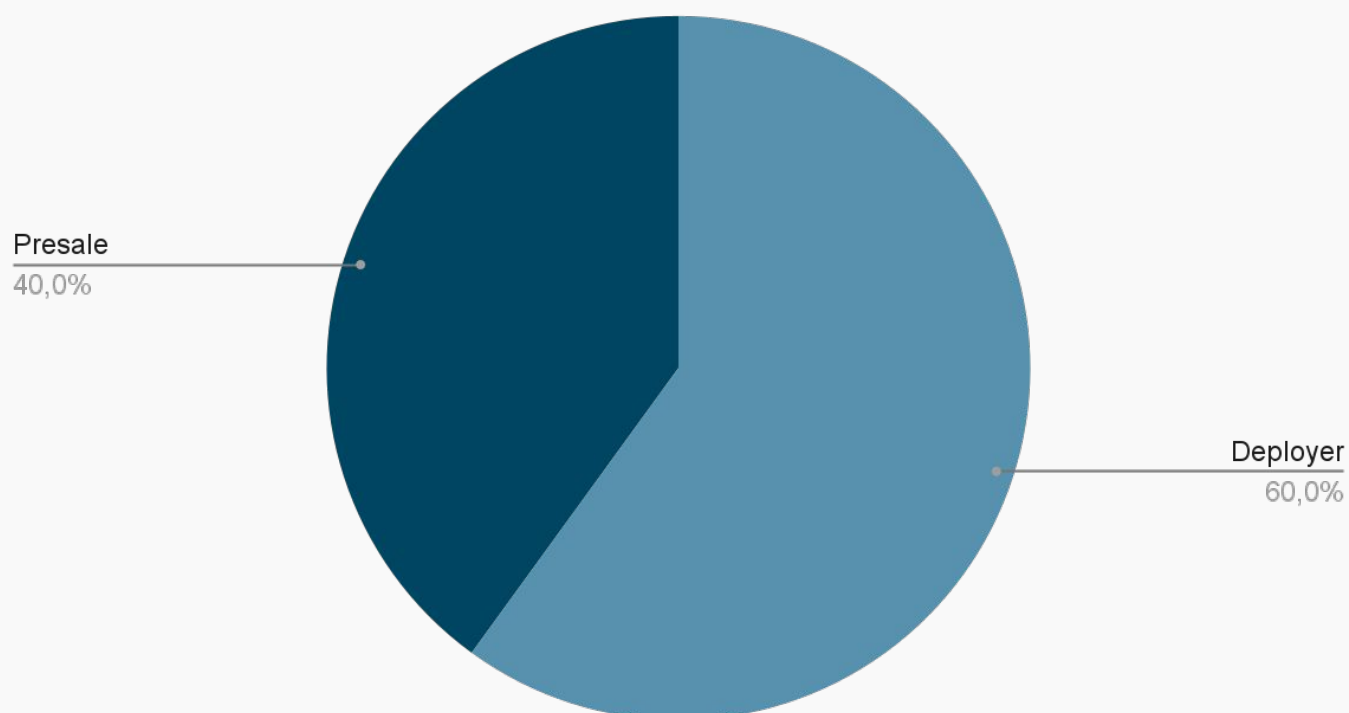
Website URL:
Unavailable

Domain Registry
https://www.godaddy.com

Domain Expiration
Unavailable

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Unavailable

Content
Unavailable

Whitepaper
Unavailable

Roadmap
Unavailable

Mobile-friendly?
Unavailable
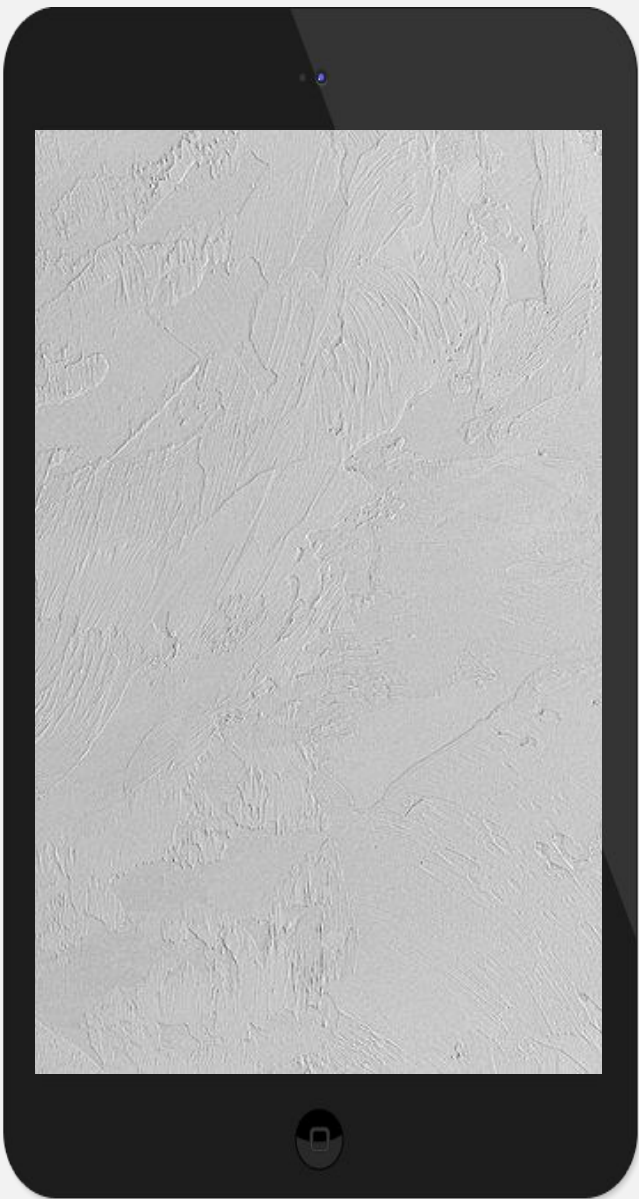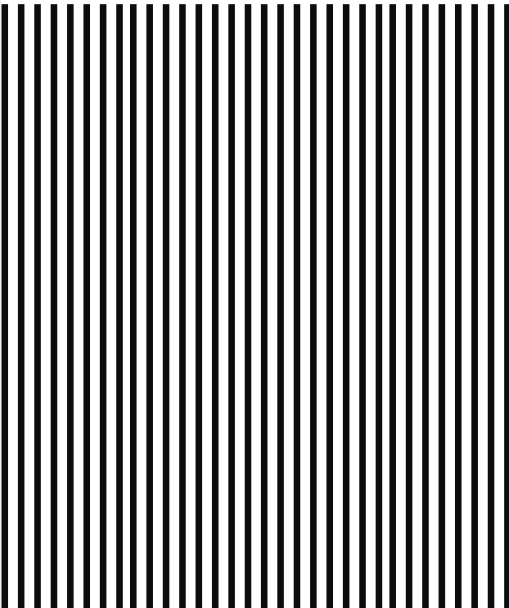
Under Construction

SOCIAL MEDIA

Social Score: 0%

ANALYSIS

No social media pages created yet

Twitter:

Unavailable

Discord

Unavailable

Telegram:

Unavailable

Medium

Unavailable

11

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 700 SUCCESSFUL CLIENTS**

- ✔ **MORE THAN 1000 SCAMS EXPOSED**

- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

✈ **@SPYWOLFNETWORK**

🐦 **@SPYWOLFNETWORK**

12

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.