



SPYWOLF

Security Audit Report



Audit prepared for
Lemon

Completed on
March 19, 2025

@SPYWOLFNWORK



@SPYWOLFNWORK



SPYWOLF.CO





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 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 -

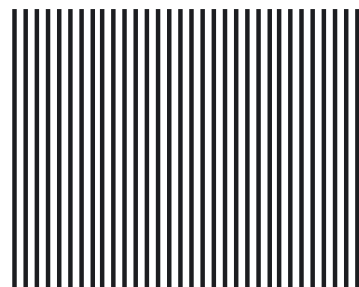
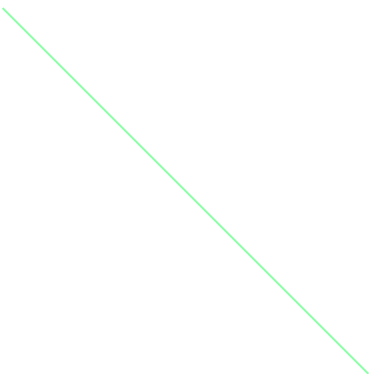




TABLE OF CONTENTS

Project Description	01
BSC Contract Information	02
Vulnerability Check	03
Found Threats	04-05
Lemon Chain Contract Information	06
Found Threats	07
Website Analysis	08
Social Media & Online Presence	09
About SPYWOLF	10
Disclaimer	11



LEMON



PROJECT DESCRIPTION

LEMON Layer 2 Projects have a crucial mission: to pioneer the digitalization and decentralization of Real World Assets (RWAs) through innovative blockchain strategies. These strategies enable businesses worldwide to seamlessly onboard and scale within the LEMON blockchain ecosystem. By leveraging advanced technology and a global community of NFT holders, LEMON fosters widespread adoption and utilization, creating the most powerful blockchain business ecosystem ever constructed.

Release Date: Launched July 15, 2024

Category: Ecosystem





BSC CONTRACT INFO

Token Name Lemon	Symbol LEMX
Contract Address 0x2Da91257961b87e69Fa13b2e20931D517dc97597	
Network Binance Smart Chain	Language Solidity
Deployment Date Jul 15, 2024	Contract Type ERC20 Token
Total Supply 50,000,000 LEMX	Status Launched

TAXES

Buy Tax
0%

Sell Tax
0%

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



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



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



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.



FOUND THREATS

High Risk

No high risk-level threats found in this contract.

Medium Risk

No medium risk-level threats found in this contract.

Low Risk

No low risk-level threats found in this contract.

The Lemon BSC contract (LEMX) has **renounced ownership**, meaning the owner address has been set to the zero address (0x00). This ensures that no one, including the original deployer, can perform privileged actions such as pausing transfers or modifying the contract. With ownership renounced, the contract operates in a fully decentralized manner, keeping everything safe from centralized control or interference, and ensuring the token's behavior remains predictable and secure for all users.



FOUND THREATS

Informational

Fixed Supply with No Minting or Burning Mechanisms

The LEMX contract on BSC has a fixed total supply of 50,000,000 tokens, minted at deployment with no additional minting or burning functions available. This ensures that the token supply cannot be inflated or reduced, providing predictability for investors. However, investors should note that this rigidity means the project cannot adjust the supply in response to market conditions or ecosystem needs, which could impact long-term flexibility.

Pausable Feature Permanently Disabled

LEMX inherits pausable functionality, allowing token transfers to be paused in emergencies, but with ownership renounced, this feature is permanently disabled. Investors should note that while this enhances decentralization by preventing centralized control, it also means the contract cannot be paused to mitigate unforeseen issues, such as exploits in external protocols interacting with LEMX, relying entirely on the token's current design for security.

Dependency on BSC Network Conditions

As LEMX operates on the Binance Smart Chain, its performance and usability are tied to BSC's network conditions, such as gas fees and transaction speeds. While BSC is known for low-cost transactions, investors should be aware that network congestion or fee spikes during high activity periods could impact the cost and speed of LEMX transfers, especially for frequent trading or interactions with dApps.



LEMON CHAIN CONTRACT INFO

Token Name Wrapped LEMX	Symbol WLEMX
Contract Address 0x84862e65EBF37aF91a8b85283B58505dE3352588	
Network Lemon Chain	Language Solidity
Deployment Date Jul 15, 2024	Contract Type Wrapped Token
Total Supply 20,340,108.131 WLEMX	Status Launched

TAXES



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



FOUND THREATS

High Risk

No high risk-level threats found in this contract.

Medium Risk

No medium risk-level threats found in this contract.

Low Risk

No low risk-level threats found in this contract.



FOUND THREATS

Informational

Dynamic Supply Based on Native Currency Deposits

The WLEMX contract's total supply, currently at 20,340,108.131 WLEMX, is not fixed and depends on the amount of native currency (the Lemon Chain's equivalent of Ether) deposited into the contract. As users deposit or withdraw native currency, the supply of WLEMX increases or decreases accordingly. Investors should be aware that this dynamic supply could impact the token's circulating supply and market dynamics, unlike a fixed-supply token.

Permissionless Design with No Administrative Control

WLEMX operates without an owner or administrative role, meaning no one can pause, upgrade, or manage the contract after deployment. While this ensures decentralization and prevents centralized interference, investors should note that there's no mechanism to address potential issues, such as recovering funds if native currency is sent to the contract outside the intended deposit function, which could lead to discrepancies in the total supply.

Dependency on Lemon Chain Network Performance

As WLEMX operates on the Lemon Chain, its usability is tied to the network's performance, including transaction fees and confirmation times. While Lemon Chain may offer benefits like low-cost transactions, investors should be mindful that network congestion, fee fluctuations, or chain-specific risks (e.g., validator centralization) could affect the cost and speed of WLEMX transactions, particularly during high activity periods or when interacting with dApps.



WEBSITE

Website URL

<https://www.allthingslemon.io/>

Domain Registry

<http://www.godaddy.com>

Domain Expiration

2026-06-10

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Very nice color scheme and overall layout.

Content

The information helps new investors understand what the product does right away. No grammar errors found. .

Whitepaper

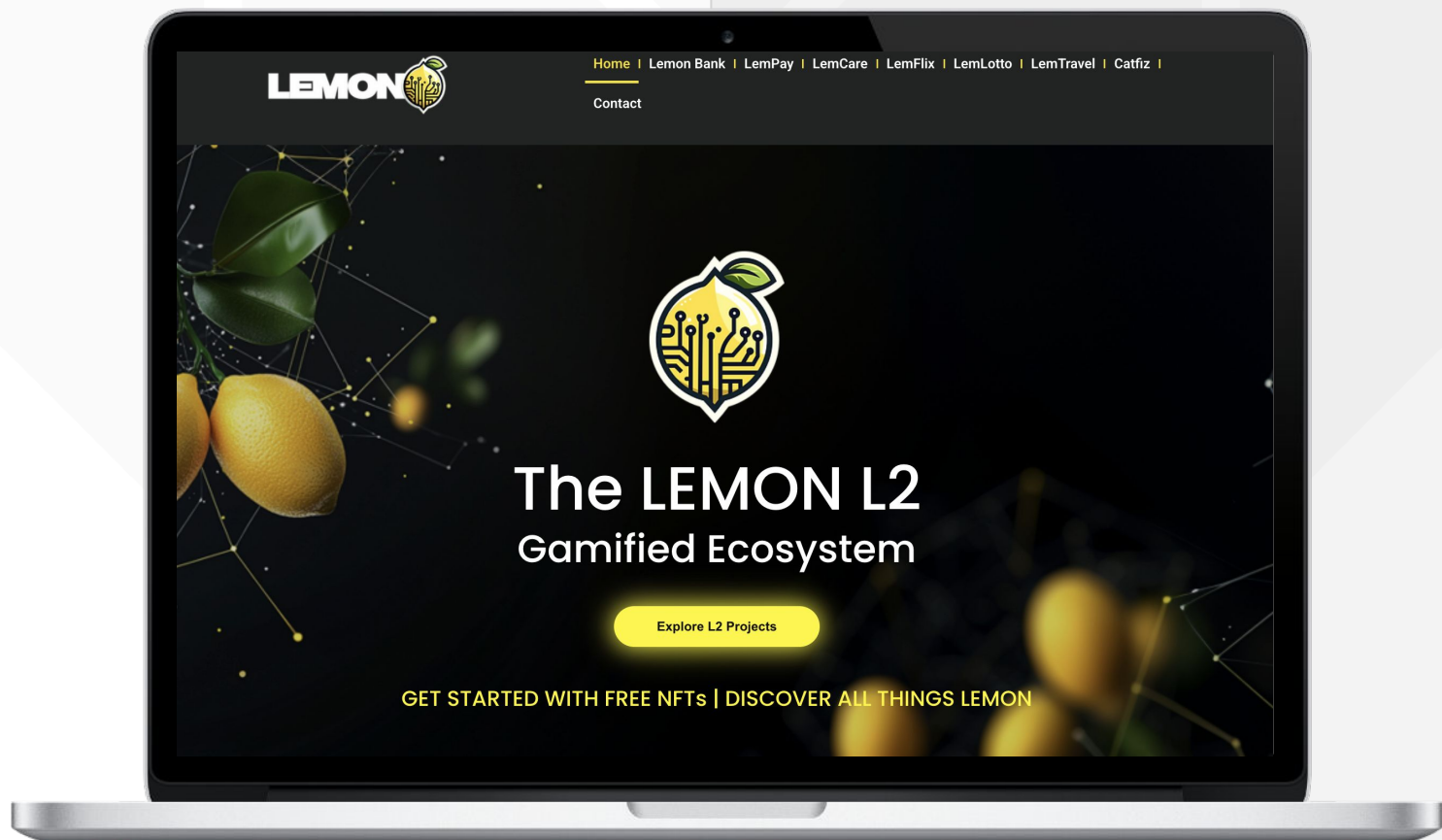
Well written but a bit short

Roadmap

Yes

Mobile-friendly?

Yes



www.allthingslemon.io

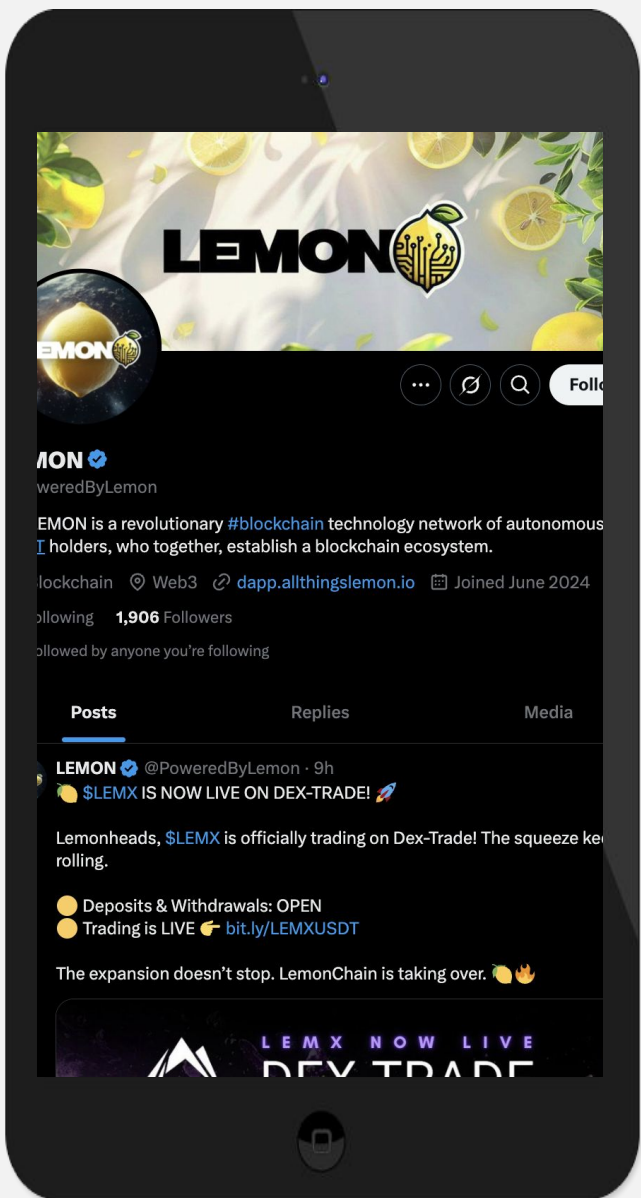
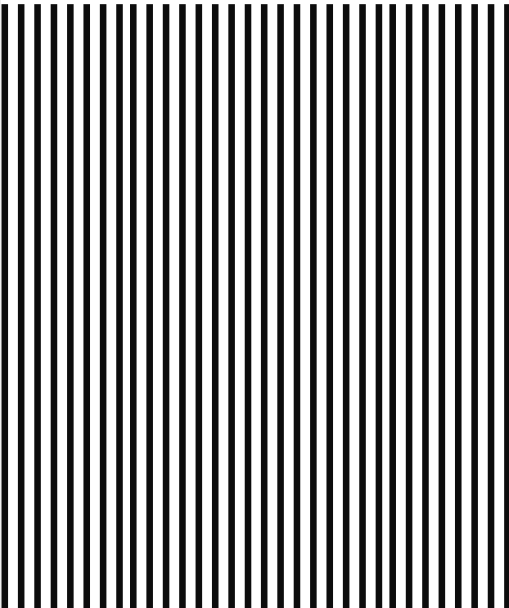


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

The project's social media pages are active with daily posts.



Twitter's X

@PoweredByLemon

- 1,906 Followers
- Responds to comments
- Daily posts



Discord

- Not available



Telegram

@AllThingsLemon

- 6 296 members
- Active mods and devs
- Daily announcements



Medium

- Not available



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](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



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.