SPYWOLF

Security Audit Report

Audit prepared for

LiquidChain

Completed on

November 12, 2025

SPYWOLF.CO @SPYWOLFNETWORK @SPYWOLFNETWORK

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	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.

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

Project Description	01
Contract Information	02
Vulnerability Check	03
Errors Found	04
Manual Code Review	05
Findings	06
Conclusion	07
Website Analysis	08
Social Media & Online Presence	09
About SPYWOLF	10
Disclaimer	11

LIQUIDCHAIN

PROJECT DESCRIPTION

LiquidChain is a new type of blockchain layer (an L3) that connects Bitcoin, Ethereum, and Solana into one single, unified system. Think of it as a superhighway for crypto capital, allowing liquidity and dApps from all three ecosystems to work together seamlessly for the first time.

Release Date: Presale starts Nov 11, 2025

Category: Token

CONTRACT INFO

Token Name
LiquidChain

Symbol
LIQUID

Contract Address
0x174b9Bb290D5CcAEa7F2517484f1Fd8e7Dc1f591

Network
Ethereum Mainnet

Language
Solidity

Deployment Date
Oct-29-2025

Contract Type
Standard Token

Total Supply
11,800,000,100

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

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.

FINDINGS

Low Risk

Unrestricted Burn Functionality (ERC20Burnable)

Because the token extends ERC20Burnable, **any holder can burn their own tokens**.

This is not unsafe, but it introduces:

- **Supply volatility**
- Potential integration issues for systems assuming a non-burnable ERC20

Not an exploit — but this changes token behavior.

FINDINGS

Low Risk

Large Constants Increase Bytecode Size

The contract stores several large uint256 public constant values:

```
uint256 public constant aquaVaultReserve = 1_770_000_015 ether;
```

This is safe, but:

- Increases bytecode size
- Slightly increases deployment cost

Still not dangerous — purely a technical/ecosystem consideration.

FINDINGS

Low Risk

No Events Emitted for Mints in Constructor

The contract stores several large uint256 public constant values:

OpenZeppelin's _mint does emit a Transfer(address(0), recipient) event — so technically events *are* emitted.

However:

- There is **no custom event** documenting allocation intent
- This is purely informational
- No impact on safety or functionality

FINDINGS

Low Risk

No Override of decimals()

Token uses OpenZeppelin's default **18 decimals**, which is standard, but:

- Some ecosystems expect explicit declaration
- Zero risk — purely stylistic

FINDINGS

Informational

1. No Honeypot Logic

The token does **not** contain:

- Max wallet limits
- Max transaction limits
- Cooldown timers
- Transfer blocking
- DEX/router logic
- Conditional taxes
- Fee collection logic
- “OnlyDEX” sell checks
- Backdoor restrictions

2. No Minting After Deployment

All minting occurs **only inside the constructor**.

After deployment:

- No function exists that mints more tokens
  Total supply is immutable

3. Not Upgradeable

The contract:

- Uses a real constructor
- Has no proxy pattern
- Has no upgrade hooks

The logic is permanently fixed.

4. Fully Based on OpenZeppelin 5.4.0

This is a strong positive:

- Widely audited
- Security-hardened
- Safe math by default
- Prevents overflows/underflows

CONCLUSION

The **LiquidChainToken** contract is a minimal, standard ERC-20 implementation built on top of OpenZeppelin 5.4.0. It contains **no malicious logic, no hidden owner privileges, no minting functions beyond deployment, no taxes, no blacklists, no pausing, no trading restrictions, no upgradeability, and no rug-enabling mechanisms**. From a pure smart-contract perspective, the code is clean, transparent, and functions exactly as a standard ERC-20 + Burnable token should.

All findings within the codebase show **no high-severity vulnerabilities**, and only minor informational notes typical of simple ERC-20 contracts. There are **no technical attack surfaces** such as reentrancy, external call vectors, proxy backdoors, or unsafe arithmetic.

The **only meaningful risks relate to centralization of supply and wallet distribution**, which exist **outside** the smart-contract logic and **cannot be evaluated or controlled by the code** itself. These are economic/trust risks rather than technical ones.

In summary, the contract code itself is secure, minimal, and non-malicious, with the only real risks coming from centralization factors outside the scope of the contract.

WEBSITE

Website URL
https://liquidchain.com/

Domain Registry
http://www.godaddy.com

Domain Expiration
4/30/2027

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

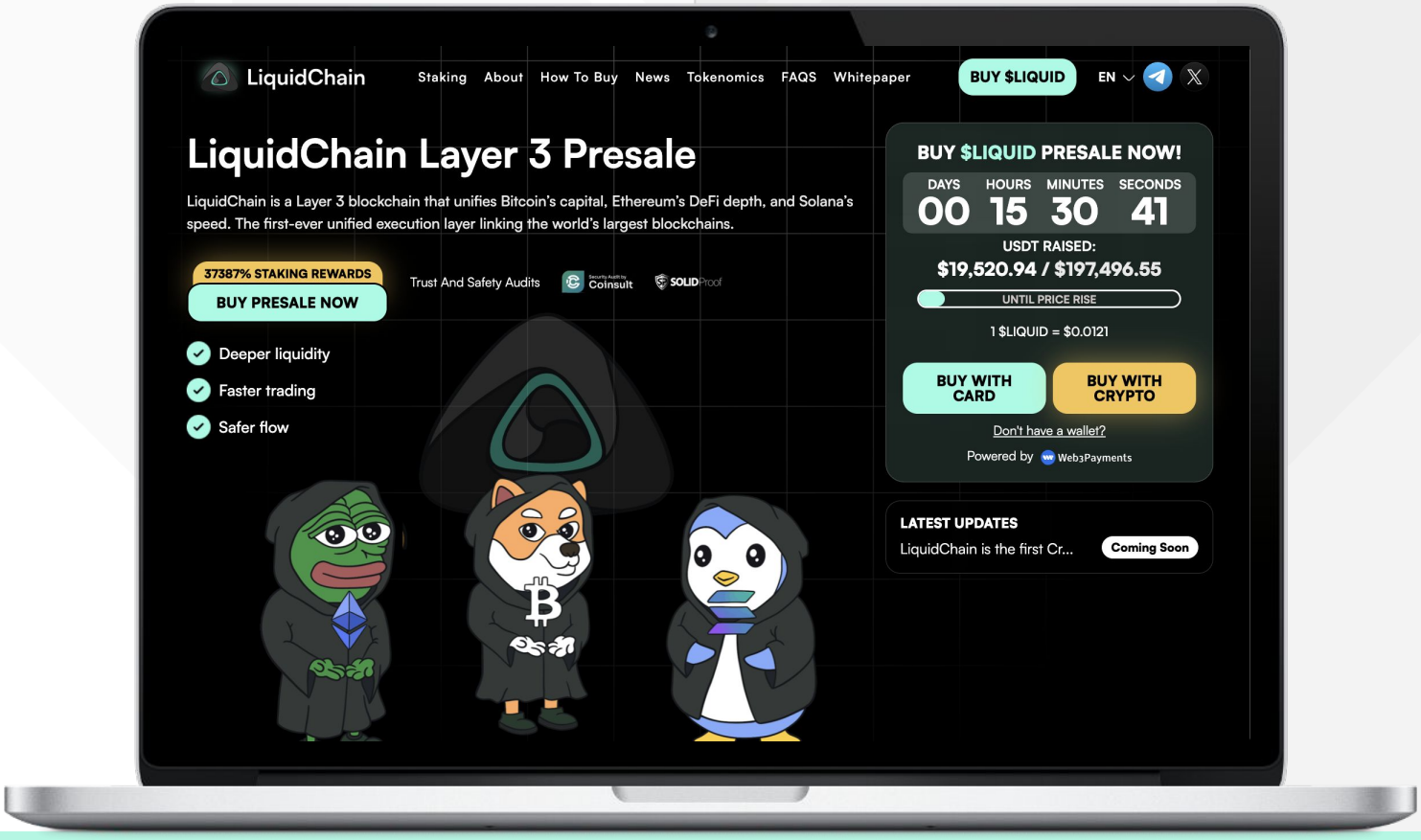
Design
Very nice color scheme and overall layout.

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

Whitepaper
Well written

Roadmap
Yes

Mobile-friendly?
Yes



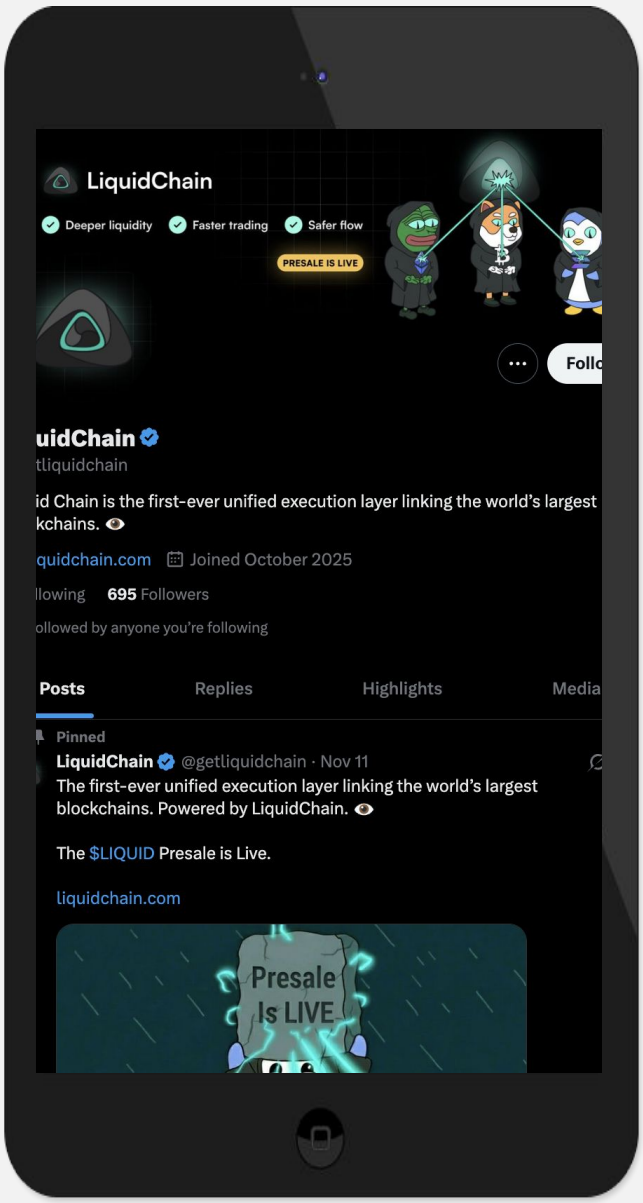
liquidchain.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

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



Twitter's X

@getliquidchain

- 695 Followers
- Responds to comments
- Daily posts

Discord

- Not available

Telegram

@liquid_chain

- 436 subscribers
- Active mods and devs
- Daily announcements

Medium

- Not available

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**

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

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

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@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.