# SPYWOLF

## Security Audit Report


Audit prepared for

**ARC**

Completed on

**August 31, 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

# ARC


## PROJECT DESCRIPTION:

ARC is the world's first Web3 intelligent computing financial platform built on an integrated smart computation network.
It also stands as the first automated, interference-free financial services platform.
ARC's mission is to leverage intelligent computation and blockchain smart contracts to create a global, permissionless platform for financial arbitrage, enabling users to maximize returns in a secure, transparent, and efficient environment.

**Release Date:** August 25TH, 2024

**Launchpad:** Fairlaunch

**Category:** DeFi

# KEY RESULTS

| | |
|---|---|
| Cannot mint new tokens | PASSED |
| Cannot pause trading (honeypot) | * |
| Cannot blacklist an address | PASSED |
| Cannot raise taxes over 25%? | PASSED |
| No proxy contract detected | NOT 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.

N/A = Not applicable for this type of contract

*Contract may turn to honey pot if call to the external ‘liquidity’ contract fails or return wrong data

# CONTRACT INFO

| | |
|---|---|
| Token Name<br>TokenARC | Symbol<br>ARC |
| Contract Address<br>0x8689de8f26d044Ac4FdD9198Fb21034Fc0f00538 | |
| Network<br>BSC | Language<br>Solidity |
| Deployment Date<br>Aug 25, 2024 | Contract Type<br>Proxy |
| Total Supply<br>5,100,000 | Decimals<br>18 |

# TAXES

| Buy Tax | Sell Tax |
|---|---|
| 3.5% | 3.5% |

# 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

# SMART CONTRACT STATS

| | |
|---|---|
| **Calls Count** | 2473 |
| **External calls** | 247 |
| **Internal calls** | 2226 |
| **Transactions count** | 842 |
| **Last transaction time** | 2024-08-31 08:37:39 UTC |
| **Deployment Date** | 2024-08-25 03:54:19 UTC |
| **Create TX** | 0x1ea2b481b3cea8805f3e3d4dbdce1c7cdceb3518b4573911d687e240af536d9a |
| **Owner** | 0x2b6d062103f245e87a5fb131b8bd57175f74bdfe |
| **Deployer** | 0x2b6d062103f245e87a5fb131b8bd57175f74bdfe |

# TOKEN TRANSFERS STATS

| | |
|---|---|
| **Transfer Count** | 2285 |
| **Total Amount** | 10618982.829647196 ARC |
| **Median Transfer Amount** | 5.792585646713689 ARC |
| **Average Transfer Amount** | 4647.2572558631055 ARC |
| **First transfer date** | 2024-08-25 |
| **Last transfer date** | 2024-08-31 |
| **Days token transferred** | 7 Days |

# FEATURED WALLETS

| | |
|---|---|
| **Owner address** | Ownership is renounced<br>0x0000000000000000000000000000000000000000 |
| **Marketing fee receiver** | 0x0000000000000000000000000000000000000000 |
| **LP address** | **Pancakeswap:**<br>0x4639372908f42E8619cFa0591eec74D3bd2956C1<br><br>**90.8% unlocked, held by token's deployer**<br>0x2b5Bd349c4bbe540a6679c1e015f77EA71AC5B51 |

# TOP 3 UNLOCKED WALLETS

| | |
|---|---|
| **92,13%** | Proxy contract<br>0x3e66B7B346aC6916700DA0Bf7bBF43d9AEbF7C8D |
| **2%** | 0xF770870Eb0E8E72E7507Cca7bF078097F1f7d982 |
| **1%** | Proxy contract<br>0x93DFf6BA0E48C52171c1Da5b5B535BC3F9AA9cC4 |

# 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.

**Code Score: 50%**

# FOUND THREATS

## High Risk: 0

No high risk-level threats found in this contract.

## Medium Risk: 2

See the next page for explanation on risks

## Low Risk: 0

No low risk-level threats found in this contract.

Current token’s implementation ownership is renounced.
Owner cannot use only owner functionalities.

# FOUND THREATS

## ⚠ Medium Risk

**This is proxy contract.**
Proxy contract's logic can be changed in time, effectively changing the current token functions/logic.
This may lead to undesirable results for investors.

Address stated in slide 02 - CONTRACT INFO,  is of the proxy contract (0x8689de8f26d044Ac4FdD9198Fb21034Fc0f00538)

The current audit is for proxy contract's implementation (token) at address (0x3aac62Ce68197643a9647971cA2e1c1D818a90f0)

# FOUND THREATS

## ⚠ Medium Risk

External call is made to distributeTradeFeeForLiquidity function of the 'liquidity' contract address.
If 'liquidity' contract's function call fails, the entire transaction will fail, effectively turn the token contract into honeypot.
If 'liquidity' contract return value higher than toDistribute's value, overflow will occur, causing the transaction to fail - effectively turn the token contract into honeypot.

Current 'liquidity' contract is proxy contract and its logic can be altered over time.
***'liquidity' contract logic is not in the scope of the current audit.***

```
function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.....................
if (liquidityFee > 0) {
super._transfer(from, address(this), liquidityFee);
    amount -= liquidityFee;

    uint256 toDistribute = liquidityFee + tokensForLiquidity;
    super._approve(address(this), liquidity, toDistribute);
    uint256 distributed = IMining(liquidity).distributeTradeFeeForLiquidity(toDistribute);
    tokensForLiquidity = toDistribute - distributed;
}
.....................
}
```

- Recommendation:
  - Considered as good practice is calls to external contracts to be wrapped in try{} catch{} statement

# FOUND THREATS

## Informational: 3

'dev' address can withdraw accumulated dev taxes from the contract

```
function claimTradeFeeForDev() external returns (uint256) {
    require(msg.sender == dev, 'permission deny');
    uint256 _tokensForDev = tokensForDev;
    tokensForDev = 0;
    if (_tokensForDev > 0) {
        super._transfer(address(this), dev, _tokensForDev);
    }
    return _tokensForDev;
}
```

'liquidity' address can withdraw accumulated liquidity taxes from the contract.

```
function claimTradeFeeForLiquidity() external returns (uint256) {
    require(msg.sender == liquidity, 'permission deny');
    uint256 _tokensForLiquidity = tokensForLiquidity;
    tokensForLiquidity = 0;
    if (_tokensForLiquidity > 0) {
        super._transfer(address(this), liquidity, _tokensForLiquidity);
    }
    return _tokensForLiquidity;
}
```

# FOUND THREATS

## Informational: 3

0.5% of liquidity pair's token supply is burnt once per 24 hour

```
function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.........................
if (
        !isAddLiquidity &&
        !swapping &&
        !automatedMarketMakerPairs[from] &&
        !_isExcludedFromFees[from] &&
        !_isExcludedFromFees[to]
    ) {
        swapping = true;

        if (
            automatedMarketMakerPairs[to] &&
            lpBurnEnabled &&
            block.timestamp >= lastLpBurnTime + lpBurnFrequency &&
            canBurn
        ) {
            autoBurnLiquidityPairTokens();
        }
        swapping = false;
    }
.........................
}

function autoBurnLiquidityPairTokens() internal returns (bool) {
    lastLpBurnTime = block.timestamp;
    // get balance of liquidity pair
    uint256 liquidityPairBalance = balanceOf(uniswapV2Pair);
    // calculate amount to burn
    uint256 amountToBurn = liquidityPairBalance.mul(percentForLPBurn).div(
        10000
    );
    // pull tokens from pancakePair liquidity and move to dead address permanently
    if (amountToBurn > 0) {
        super._transfer(uniswapV2Pair, deadAddress, amountToBurn);
    }
    //sync price since this is not in a swap transaction!
    IUniswapV2Pair(uniswapV2Pair).sync();
    emit AutoNukeLP();
    return true;
}
```

The following tokenomics are based on BSCScan:

Tokenomics:

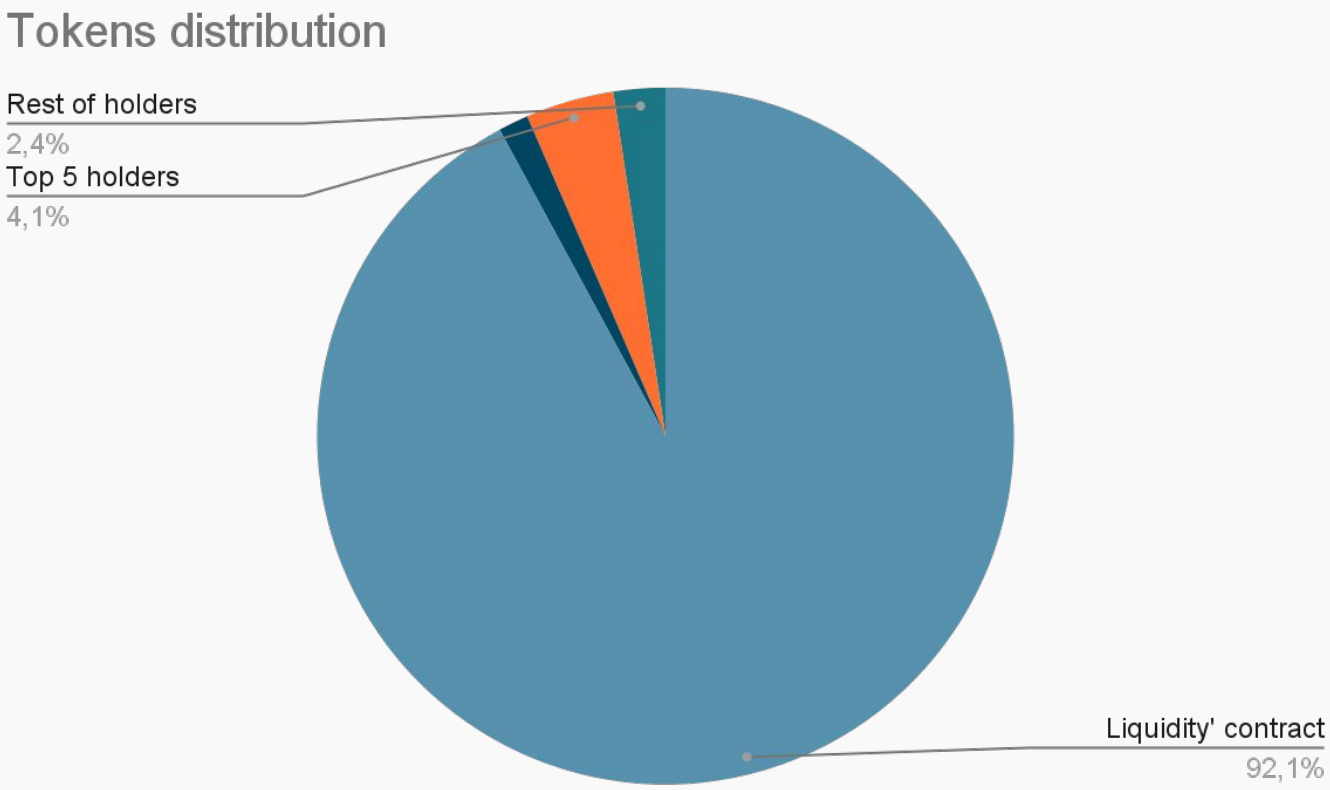
‘Liquidity’ contract - 92.1%,

Liquidity pair - 1.4%,

Top 5 holders - 4.1%,

Rest of holders - 2.4%,

## Token Distribution




TOKENOMICS

# WEBSITE

**Website URL:**
https://arcfinance.net/

**Domain Registry**
https://registrar.amazon.com

**Domain Expiration**
2025-08-02

**Technical SEO Test**
Passed

**Security Test**
Passed. SSL certificate present

**Design**
Single page design with appropriate color scheme and graphics.

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

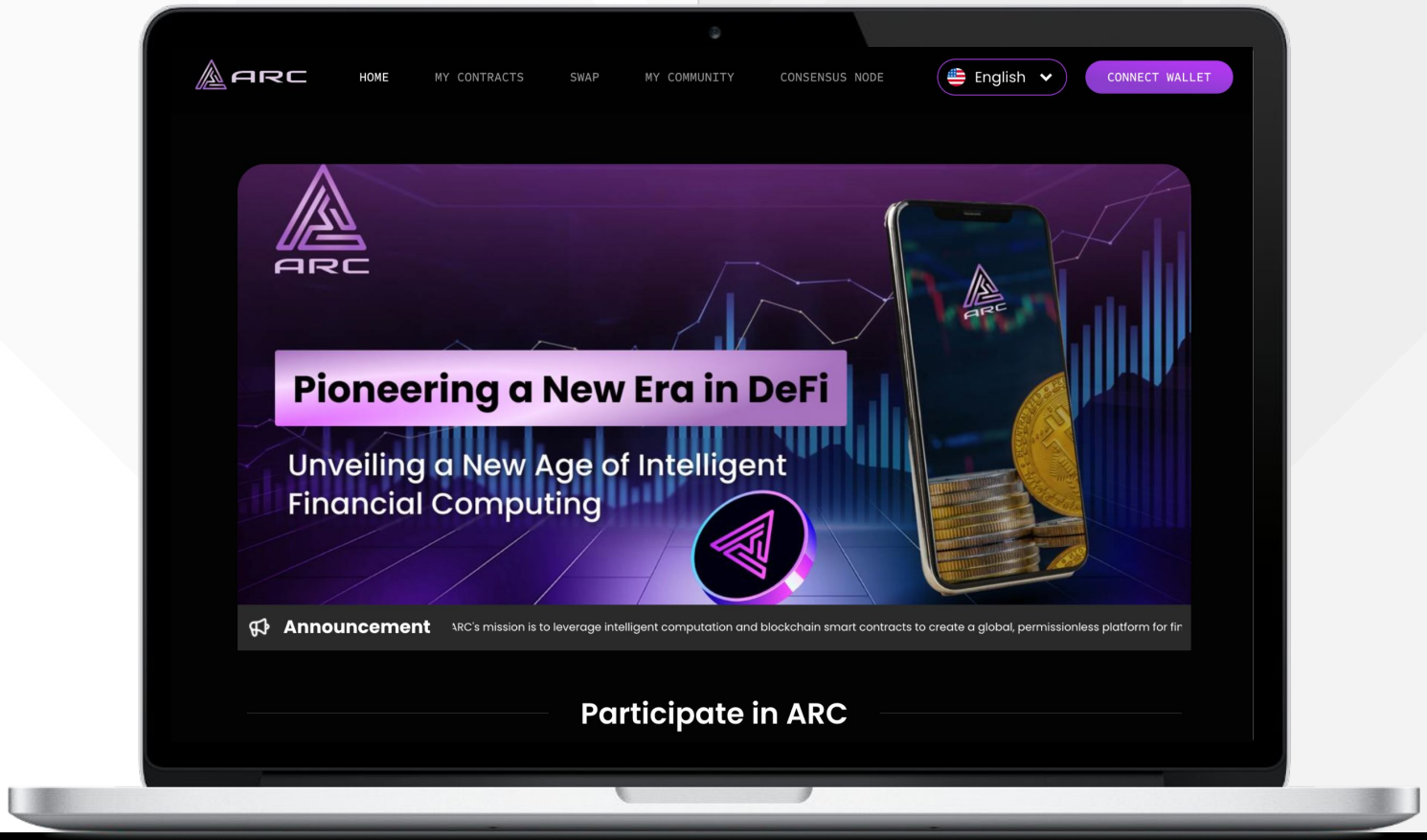
**Whitepaper**
No

**Roadmap**

No

**Mobile-friendly?**

Yes



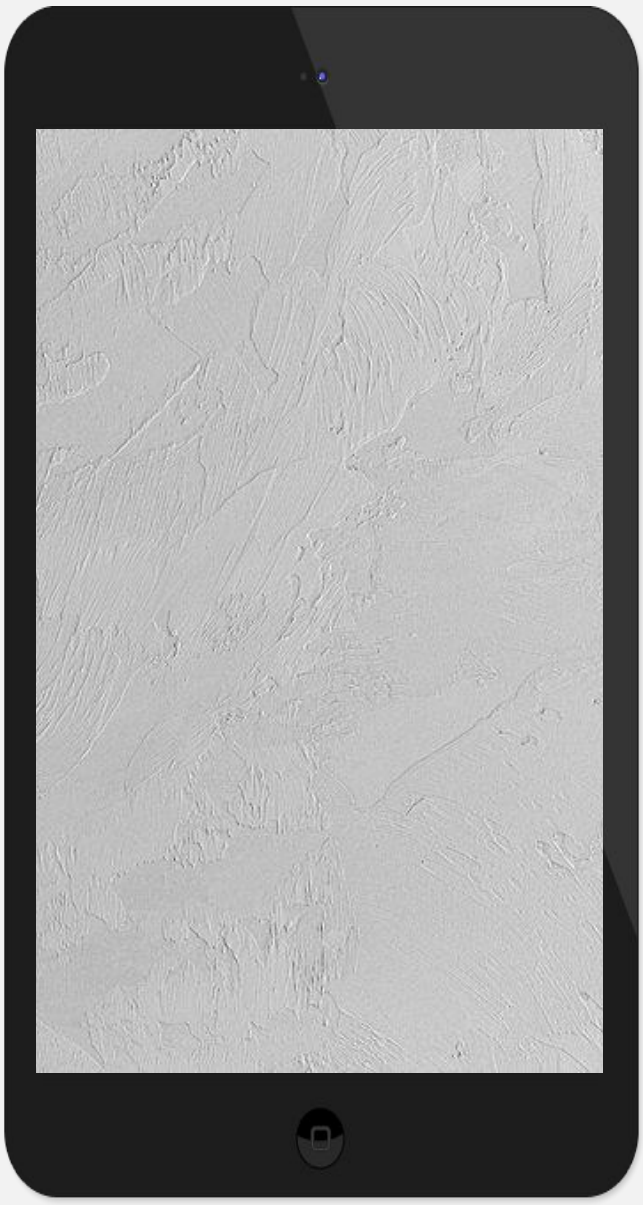

**Website Score: 100%**

# SOCIAL MEDIA

## Social Score: 0%

**ANALYSIS**

**Project is not present in social medias**



**Twitter:**

unavailable

**Discord**

unavailable

**Telegram:**

unavailable

**Medium**

unavailable

# 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

# 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.