SPYWOLF

Security Audit Report

Audit prepared for

DESCITRUMP

Completed on

January 10, 2025

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

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.

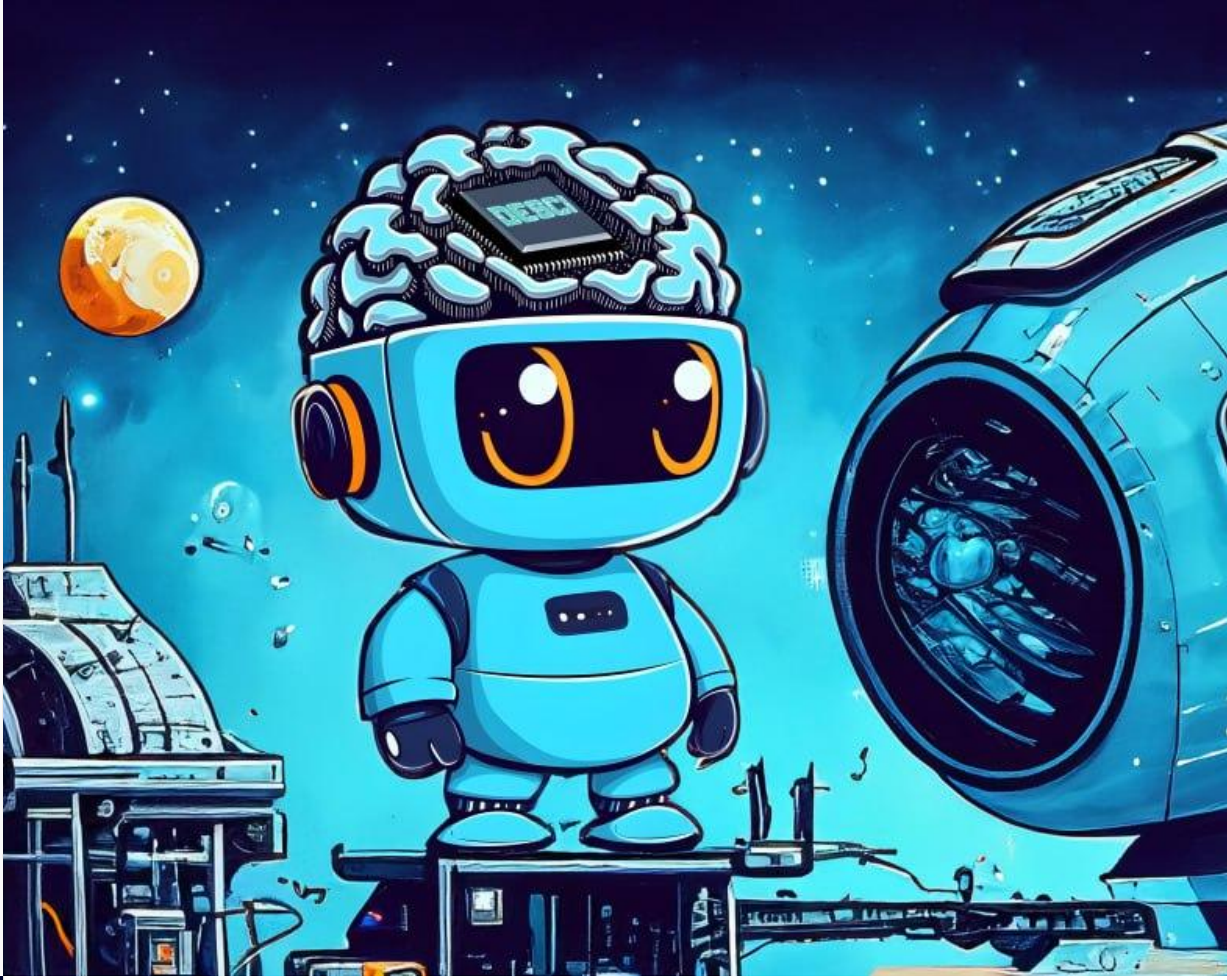
You will find a a summarized review of the following key points:

- ✓ 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

DESCITRUMP



PROJECT DESCRIPTION:

According to their website:
A DesciAI app will provide each trader with a virtual assistant, helping to look up scientific knowledge and investment or calculate business risks conveniently.
Staking tokens to receive tokens is a thing of the past, now DesciTrump allows you to submit your scientific research achievements, or your business manuals and get paid after a while we roll that knowledge out to our readers - readers and advertisers will pay.

Release Date: Jan 14, 2025

Launchpad: Pinksale

Category: DeFi

KEY RESULTS

Cannot mint new tokens	PASSED
Cannot pause trading (honeypot)	NOT PASSED
Cannot blacklist an address	PASSED
Cannot raise taxes over 25%?	NOT 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.

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

CONTRACT INFO

Token Name
DESCITrump

Symbol
DESCITRUMP

Contract Address
0x140d1fbd93a5aB4e83D8cB2b95937c0D9bdd49e6

Network
BSC

Language
Solidity

Deployment Date
Jan 10, 2025

Contract Type
Regular token

Total Supply
1,000,000,000

Decimals
9

TAXES

Buy Tax
2%

Sell Tax
2%

*Taxes can be changed in future

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	14
External calls	2
Internal calls	12
Transactions count	6
Last transaction time	2025-01-10 12:39:04 UTC
Deployment Date	2025-01-10 11:36:16 UTC
Create TX	0x39392f916f001d866e098927bfa1834aac8ca257eccfe7138f4455b632a75c74
Owner	0x243a148457bd35544f8540bafb3000e40a5724f8
Deployer	0x243a148457bd35544f8540bafb3000e40a5724f8

TOKEN TRANSFERS STATS

Transfer Count	5
Total Amount	1180000000 DESCITRUMP
Median Transfer Amount	49000000 DESCITRUMP
Average Transfer Amount	236000000 DESCITRUMP
First transfer date	2025-01-10
Last transfer date	2025-01-10
Days token transferred	1 Days

FEATURED WALLETS

Owner address	0x243a148457bd35544f8540bafb3000e40a5724f8
Marketing fee receiver	0x243a148457bD35544F8540BaFb3000E40a5724F8
LP address	**Pancakeswap:** 0x93e897d17A8a3B2694Acd2C45c9F457EB34bD971 Liquidity is not added yet

TOP 3 UNLOCKED WALLETS

82%	Same as owner Tokens are not distributed yet 0x243a148457bD35544F8540BaFb3000E40a5724F8
unavailable	
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

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.

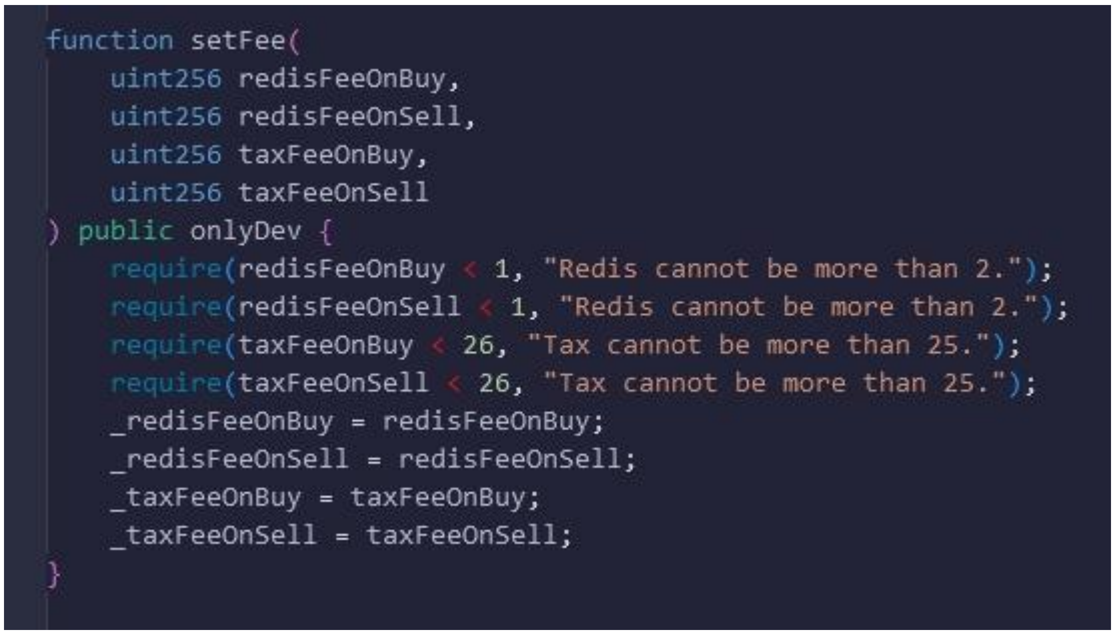
Informational

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

FOUND THREATS

⚠ Medium Risk

The contract owner is authorized to configure buy and sell fees, with each individually capped at a maximum of 25%. The combined total of buy and sell fees will not exceed 50%.



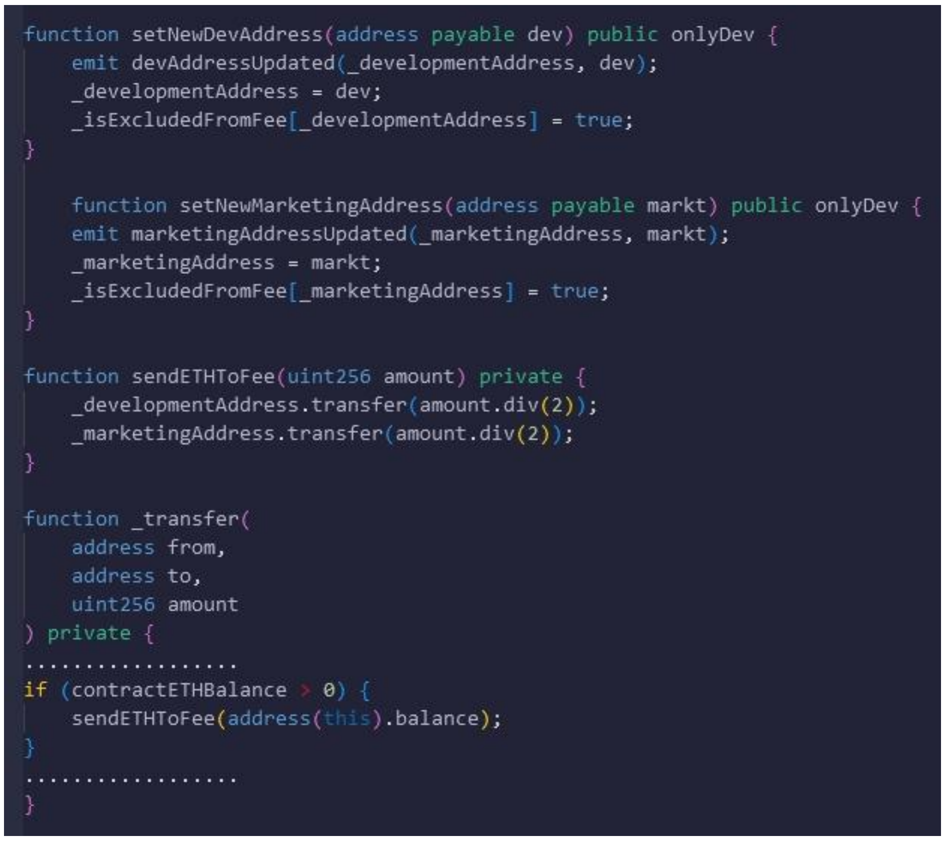
```
function setFee(
    uint256 redisFeeOnBuy,
    uint256 redisFeeOnSell,
    uint256 taxFeeOnBuy,
    uint256 taxFeeOnSell
) public onlyDev {
    require(redisFeeOnBuy < 1, "Redis cannot be more than 2.");
    require(redisFeeOnSell < 1, "Redis cannot be more than 2.");
    require(taxFeeOnBuy < 26, "Tax cannot be more than 25.");
    require(taxFeeOnSell < 26, "Tax cannot be more than 25.");
    _redisFeeOnBuy = redisFeeOnBuy;
    _redisFeeOnSell = redisFeeOnSell;
    _taxFeeOnBuy = taxFeeOnBuy;
    _taxFeeOnSell = taxFeeOnSell;
}
```

- Recommendation:
    - It is considered a best practice to ensure that the combined buy and sell fees do not exceed 25%.

FOUND THREATS

⚠ Medium Risk

The owner has the ability to update the marketing and development wallet addresses. These addresses are designated to receive BNB obtained from the swapping of collected fees within the contract. However, if _developmentAddress and/or _marketingAddress are set to addresses incapable of receiving BNB, the contract will encounter a failure during sell transactions.



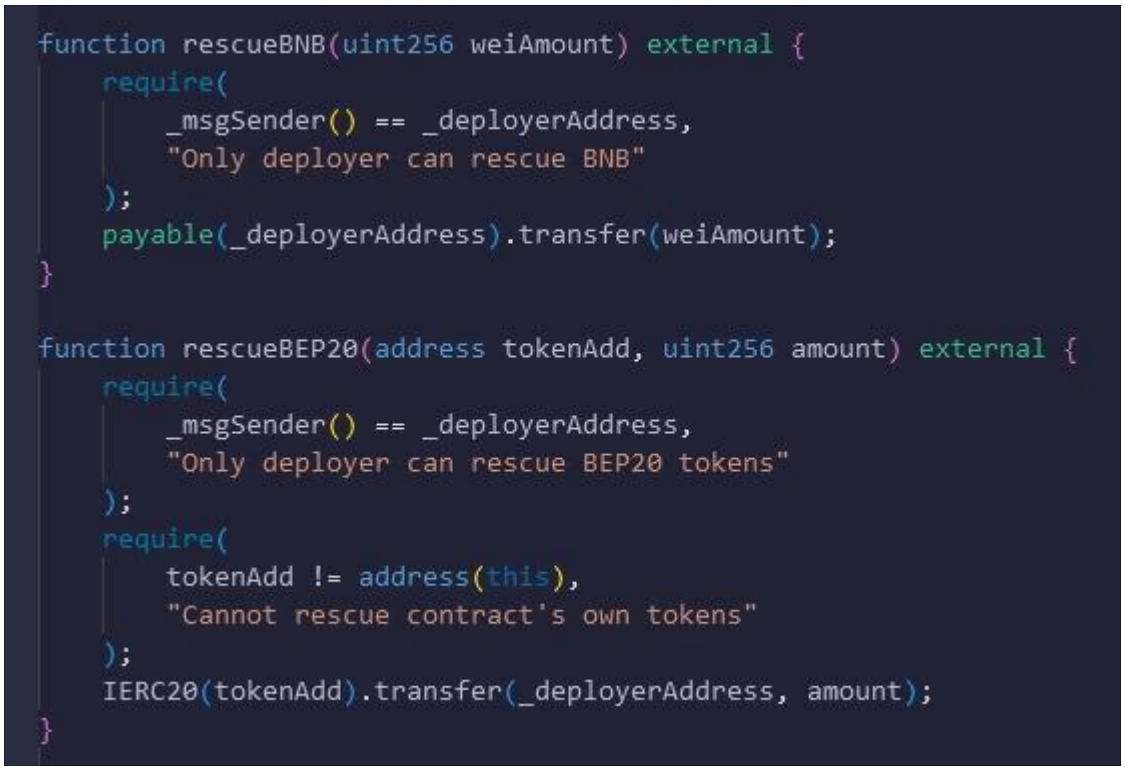
```
function setNewDevAddress(address payable dev) public onlyDev {
    emit devAddressUpdated(_developmentAddress, dev);
    _developmentAddress = dev;
    _isExcludedFromFee[_developmentAddress] = true;
}

    function setNewMarketingAddress(address payable markt) public onlyDev {
    emit marketingAddressUpdated(_marketingAddress, markt);
    _marketingAddress = markt;
    _isExcludedFromFee[_marketingAddress] = true;
}

function sendETHToFee(uint256 amount) private {
    _developmentAddress.transfer(amount.div(2));
    _marketingAddress.transfer(amount.div(2));
}

function _transfer(
    address from,
    address to,
    uint256 amount
) private {
.................
if (contractETHBalance > 0) {
    sendETHToFee(address(this).balance);
}
.................
}
```

- Recommendation:
    - It is recommended to use the .call method without specifying a gas parameter for sending BNB, rather than relying on .transfer or .send. The .call method accommodates higher gas usage and ensures that a failed BNB transfer does not cause the entire transaction to revert.

FOUND THREATS

Informational

The contract deployer has the ability to withdraw BNB and any tokens held by the contract, excluding the native DESCITRUMP token.



```
function rescueBNB(uint256 weiAmount) external {
    require(
        _msgSender() == _deployerAddress,
        "Only deployer can rescue BNB"
    );
    payable(_deployerAddress).transfer(weiAmount);
}

function rescueBEP20(address tokenAdd, uint256 amount) external {
    require(
        _msgSender() == _deployerAddress,
        "Only deployer can rescue BEP20 tokens"
    );
    require(
        tokenAdd != address(this),
        "Cannot rescue contract's own tokens"
    );
    IERC20(tokenAdd).transfer(_deployerAddress, amount);
}
```

TOKENOMICS

*The following tokenomics are based on the project's whitepaper and/or website:

Tokenomics:

Pressale - 52.5%,

Liquidity - 29.5%,

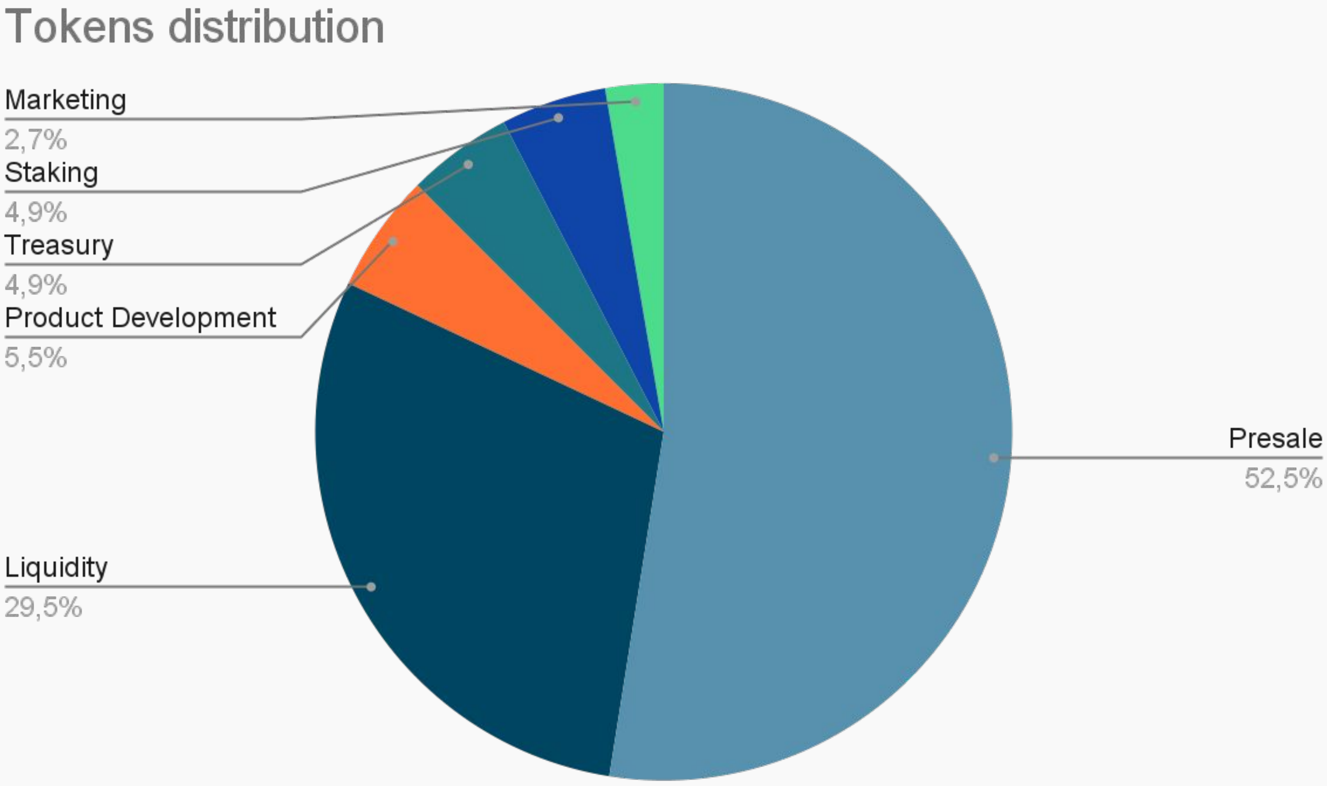
Product development - 5.5%,

Treasury - 4.9%,

Staking - 4.9%,

Marketing - 2.7%

Token Distribution



WEBSITE

Website URL:
https://descitrump.com/

Domain Registry
https://www.godaddy.com

Domain Expiration
2025-12-14

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

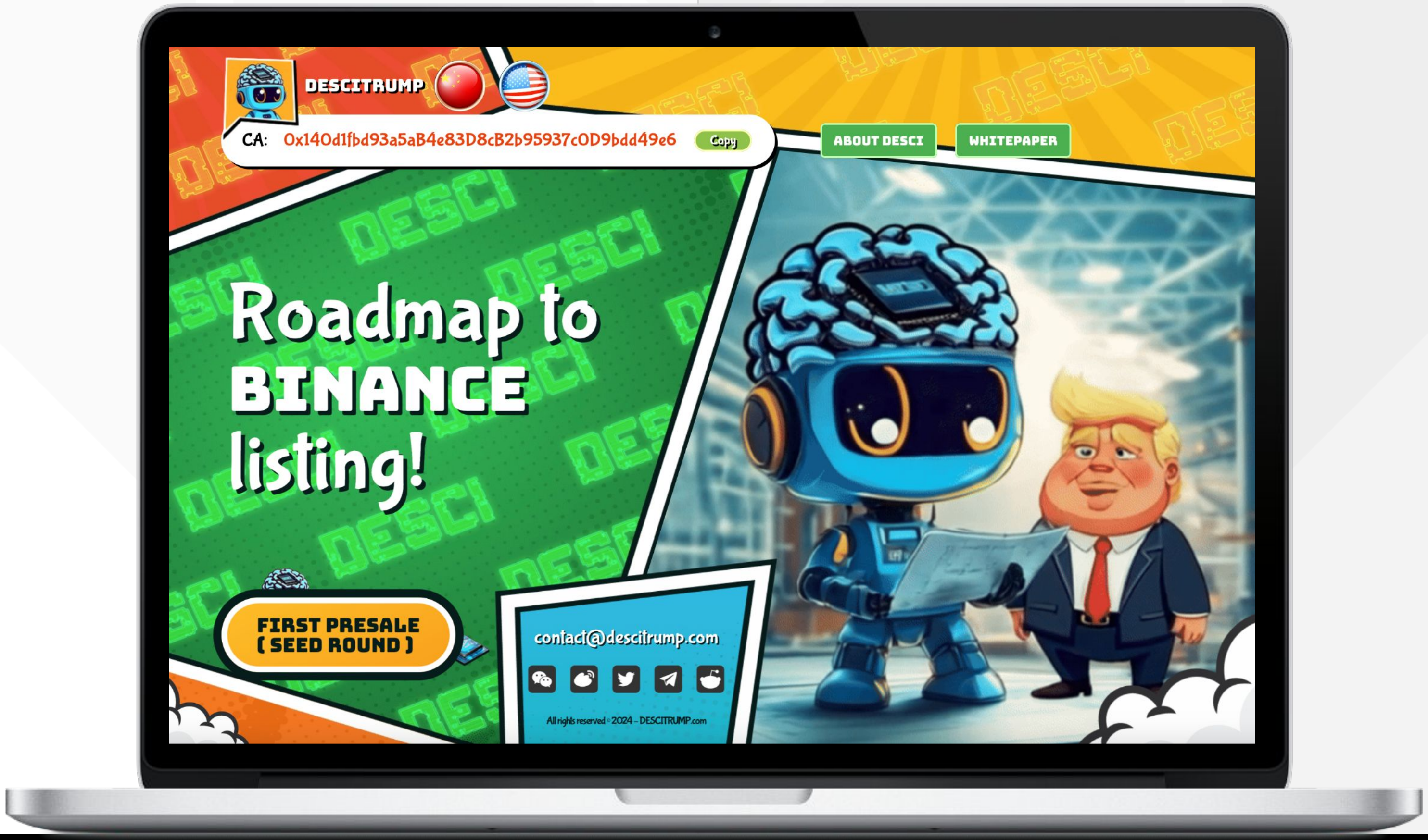
Design
Very nice color scheme and overall layout.

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

Whitepaper
Well written, explanatory

Roadmap
Yes

Mobile-friendly?
Yes


CA: 0x140d1fbd93a5aB4e83D8cB2b95937c0D9bdd49e6

Roadmap to BINANCE listing!

contact@descitrump.com

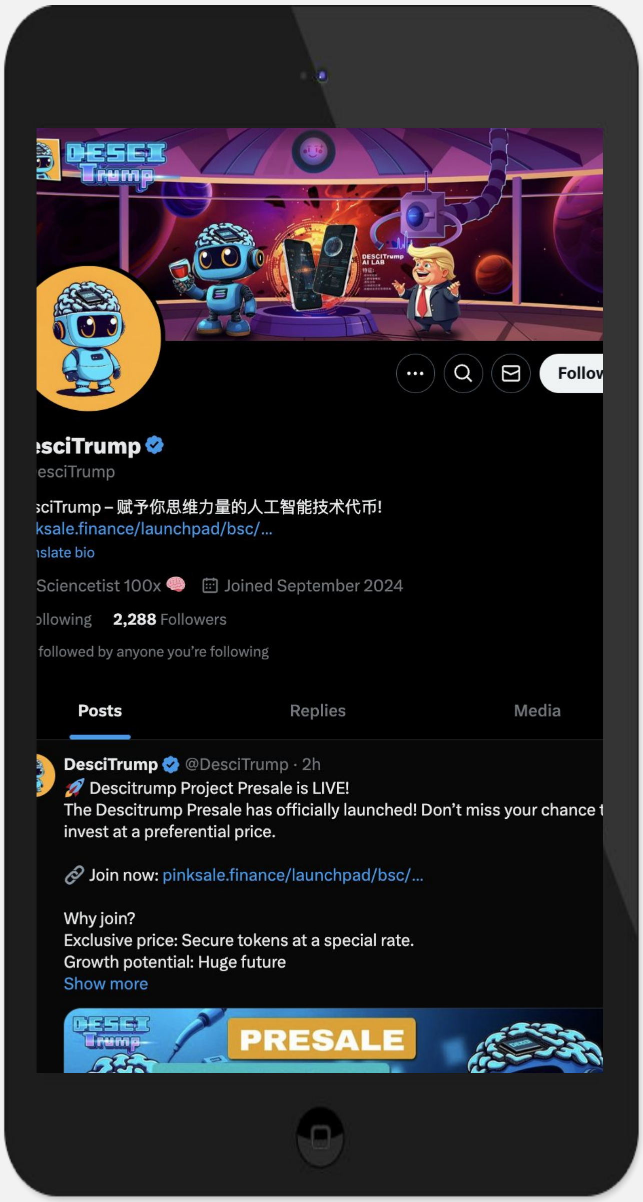
All rights reserved - 2024 - DESCITRUMP.com

descitrump.com

SOCIAL MEDIA

ANALYSIS

Project’s social media are active with daily posts.



esciTrump
esciTrump
sciTrump – 赋予你思维力量的人工智能技术代币!
ksale.finance/launchpad/bsc/...
ıslate bio
Sciencetist 100x 🧠 Joined September 2024
ollowing 2,288 Followers
followed by anyone you’re following

DesciTrump @DesciTrump · 2h
🚀 Descitrump Project Presale is LIVE!
The Descitrump Presale has officially launched! Don’t miss your chance t invest at a preferential price.

🔗 Join now: pinksale.finance/launchpad/bsc/...

Why join?
Exclusive price: Secure tokens at a special rate.
Growth potential: Huge future
Show more

Twitter:

@DESCITRUMP

- 2 305 followers
- Active
- Daily posts

Discord

Unavailable

Telegram:

@DesciCommunity

- 6 778 members
- Daily posts (channel)

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.

Final Score (hidden)

Final Score: 92

Risk Level: Low Risk

- For "Final score" only put the number without the percentage
- Input the risk levels like this:

Low Risk

High Risk

Medium Risk

SAFU