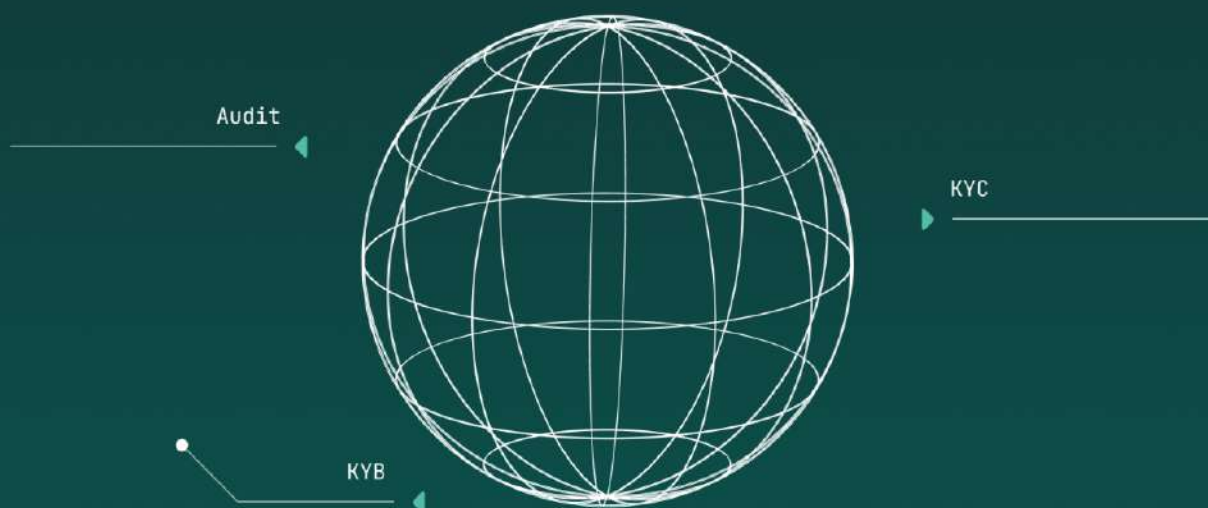




SMART CONTRACT REVIEW AND SECURITY REPORT



COMPLETED ON
JULY 11, 2022

OVERVIEW

This audit has been prepared for Instinct Coin to review their Smart Contract Code and Security. This audit report aims to help investors make an informative decision during the project research.

In this report, you will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Contract's function
- ✓ Owner's wallets
- ✓ Important Technical Stats
- ✓ Good Practices
- ✓ Recommendation

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed – upon a decision of the Customer.

- ▶ This Audit report DOES NOT guarantee nor reflect the outcome and goal of the project.
- ▶ DAudit's audit process only guarantees that the smart contract code has been verified not to have security breaches.

Table Of Content

Overview1
Contract Information2
Daudit Contract Review Process2
Project Technical Information3
Important Stats4
Vulnerability Check5
Code Review5
Function Review6
Risk Level7
Risk Found8
Good Practices Found11
About DAudit12
Disclaimer13

CONTRACT INFORMATION

Token Name	Symbol
INSTINCT	INSTINCT
Contract Name	Type
INSTINCT	ERC-20

Website

<https://instinct.love/>

Technical Documentation

[https://instinct.love/
whitepaper.pdf](https://instinct.love/whitepaper.pdf)

Contract Address

0x2967320bb05a9bb4Dd9F8198E594772B
04b458B1

Network

Binance Smart Chain

Language

Solidity

Compiler Version

v0.8.7+commit.e28d00a7

Optimization

Yes with 200 runs

Decimals

18

Total Supply

100,000,000,000

DAUDIT CONTRACT REVIEW PROCESS

Smart Contract Code review process:

- ✓ 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.

DECENTRALAB PTE.LTD.

160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org



PROJECT TECHNICAL INFORMATION

(AS OF JULY 11TH, 2022)

STATUS:

HAVEN'T LAUNCHED YET

Owner Address	0xc61b16dc0ec722e2a71d383b256d7ae38ae81cd5
Marketing Wallet	0x32035d872b39c34c458c6f2f52d94f9cc9257e82
Dead Wallet	0xc3aadd82e25ea4e759394a0d89e4f2d6f63ffa78
LP Address	0x93380025D1B4D06a7D80CC11f2F18F507ad82c84



LIQUIDITY

Status: Not added yet

IMPORTANT STATS

TAX

Buy tax: 12%
Sell tax: 12%

OWNER CAN SET FEES

Buy: Up to 100%
Sell: Up to 100%

MAX TX AMOUNT

Owner can't set max
tx amount

OWNERSHIP

Owner can renounce or
transfer ownership

MINT FUNCTION

No mint
function found

PAUSE

Owner can't
pause trading

BLACKLIST

Owner can set
blacklist

WHITELIST

Owner can set
whitelist to avoid
transaction fee

VULNERABILITY CHECK

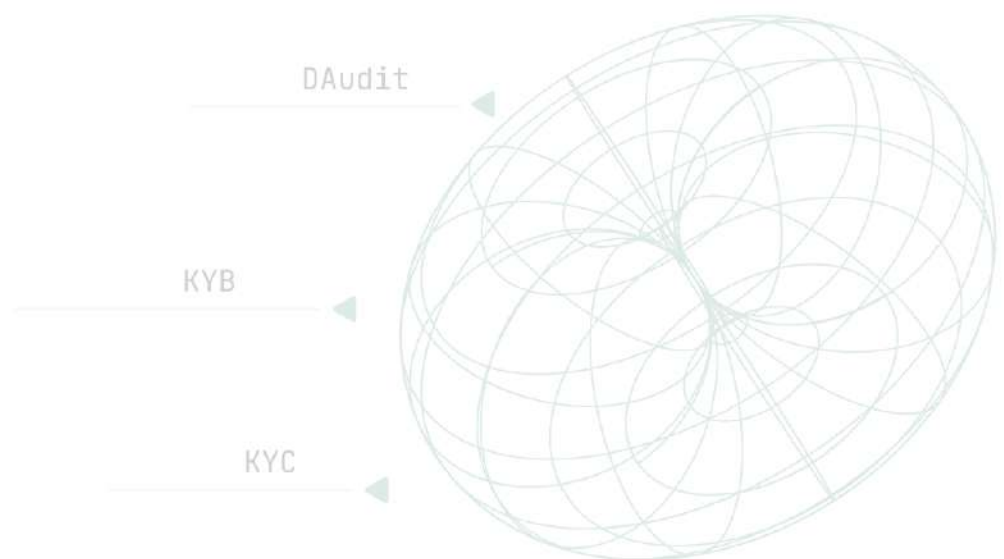
CODE REVIEW

Design Logic	Passed
Compiler Warnings	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle Calls	Passed
Front Running	Passed
DoS with block gas limit	Passed
DoS with Revert	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event Log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

VULNERABILITY CHECK

FUNCTION REVIEW

Business Logics Review Functionality Checks	Passed
Access Control & Authorization	Passed
Escrow manipulation	Passed
Token Supply manipulation	Passed
Assets integrity	Passed
User Balances manipulation	Passed
Data Consistency manipulation	Passed
Kill - Switch Mechanism Operation Trails & Event Generation	Passed



RISK LEVELS

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 the following levels:

Critical

Critical vulnerabilities are usually straightforward to exploit and can lead to asset loss or data manipulations.

High

High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions

Medium

Medium-level vulnerabilities are important to fix; however, they can't lead to asset loss or data manipulations.

Low

Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

RISK FOUND 01

CRITICAL

Owner can set blacklist user, through which any user can be prohibited from trading.

```
function multipleBotlistAddress(address[] calldata accounts, bool excluded) public onlyOwner {  
    for (uint256 i = 0; i < accounts.length; i++) {  
        _isBlacklisted[accounts[i]] = excluded;  
    }  
}
```

Recommendation:

The blacklist function should not be used because it can block a user from trading or transferring. More investors could be involved if this function was not present in smart contract.

RISK FOUND 02

CRITICAL

Owner can change total fees up to 100%. Trading fees can be set to 100%, which is inconvenient for investors who trade tokens.

```
function setBuyTaxes(uint256 marketingFee,uint256 inviterFee) external onlyOwner {  
    buyMarketingFee = marketingFee;  
    buyInviterFee = inviterFee;  
}  
  
function setSellTaxes(uint256 marketingFee,uint256 inviterFee) external onlyOwner {  
    sellMarketingFee = marketingFee;  
    sellInviterFee = inviterFee;  
}
```

Recommendation:

Total selling and buying fees should be kept at $\leq 25\%$

RISK FOUND 03

LOW

Solidity integer division might truncate. As a result, performing multiplication before division can sometimes avoid loss of precision.

```

    cur = sender;
  } else {
    super._transfer(sender, deadWallet, tAmount.div(10000).mul(sellInviterFee));
    return;
  }

```

```

    uint256 curTAmount = tAmount.div(10000).mul(rate);
    super._transfer(sender, cur, curTAmount);
  }

  super._transfer(sender, deadWallet, tAmount.div(10000).mul(sellInviterFee.sub(accurRate)));
}

```

```

  } else {
    super._transfer(sender, deadWallet, tAmount.div(10000).mul(buyInviterFee));
    return;
  }

```

```

    uint256 curTAmount = tAmount.div(10000).mul(rate);
    super._transfer(sender, cur, curTAmount);
  }

  super._transfer(sender, deadWallet, tAmount.div(10000).mul(buyInviterFee.sub(accurRate)));
}

```

Recommendation:

Consider ordering multiplication before division

INSTINCT COIN GOOD PRACTICES FOUND

1

The owner cannot mint new tokens after deployment.

2

The owner cannot stop or pause the contract.

3

The smart contract utilizes "SafeMath" to prevent overflows.

4

The owner cannot limit transaction amount.

5

The owner cannot stop or pause trading.





DECENTRALAB PTE.LTD.

160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org



ABOUT DAUDIT

DAudit offers Smart Contract vulnerability and quality testing services at a rapid pace to ensure that projects do not fall behind the market.

Experienced 	Fast 	Careful 	Affordable 
A group of experienced blockchain developers built many successful DApp applications and are familiar with security flaws.	Within 6 hours, the audit report will be on your desk! We also have professional consultation and support staff available around the clock.	We deeply analyze the smart contracts line by line and cover the smart contracts with both automated and manual testing.	Affordable We provide the most competitive price in the industry, with audit reports ranging from \$500 to \$1,000, KYC services start at \$1000, and KYB services start at \$2,000

CONTACT US

Email

support@daudit.org

Support 24/7

@daudit (Mr.Drake)

@vietdn (Mr.Viet)

daudit.org

DISCLAIMER

DAudit 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 print 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.

The smart contracts submitted for audit were examined in accordance with best industry practices at the time of this report in terms of cybersecurity vulnerabilities and issues in smart contract source code, which are detailed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no claims or guarantees about the code's security. It also cannot be deemed an adequate appraisal of the code's utility and safety, bug-free status, or any other contractual assertions. While we did our best in completing the study and generating this report, it is crucial to emphasize that you should not rely only on this report; we advocate doing many independent audits and participating in a public bug bounty program to assure smart contract security.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed

Technical Disclaimer

Smart Contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.