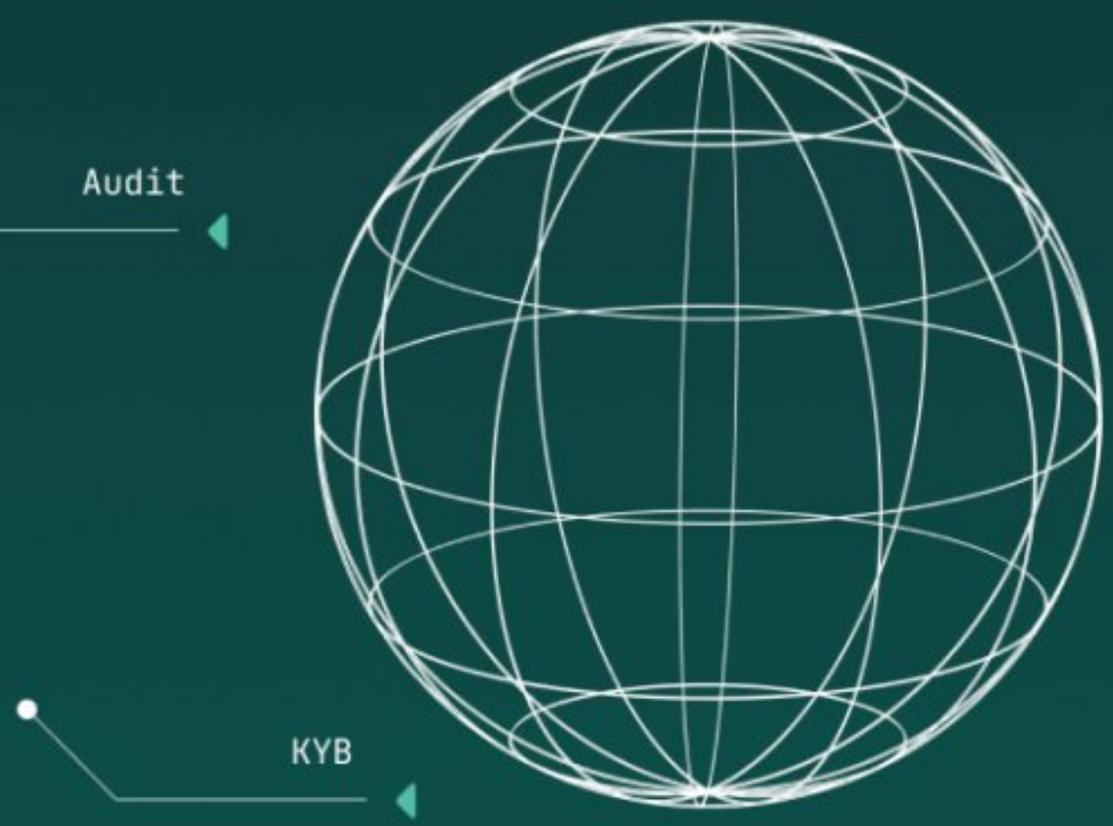
DAudit

SMART CONTRACT REVIEW AND SECURITY REPORT



COMPLETED ON

JULY 13, 2022

DAudit.org

@daudit_org

@support@dauddit.org

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

DAudit

OVERVIEW

This audit has been prepared for Bloo 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

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

DAudit

Table Of Content

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

DAudit

CONTRACT INFORMATION

Token Name
BLOO

Symbol
BLC

Contract Name
BLOO

Type
ERC-20

Website
https://bloocoin.org/

Technical Documentation
https://docs.bloocoin.org/

Contract Address
0xd56d87bF632181f8E2B8a800dc75ceD87a2b9757

Network
Polygon

Language
Solidity

Compiler Version
v0.8.13+commit.abaa5c0e

Optimization
Yes with 777 runs

Decimals
18

Total Supply
480,000 BLC

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

DAudit

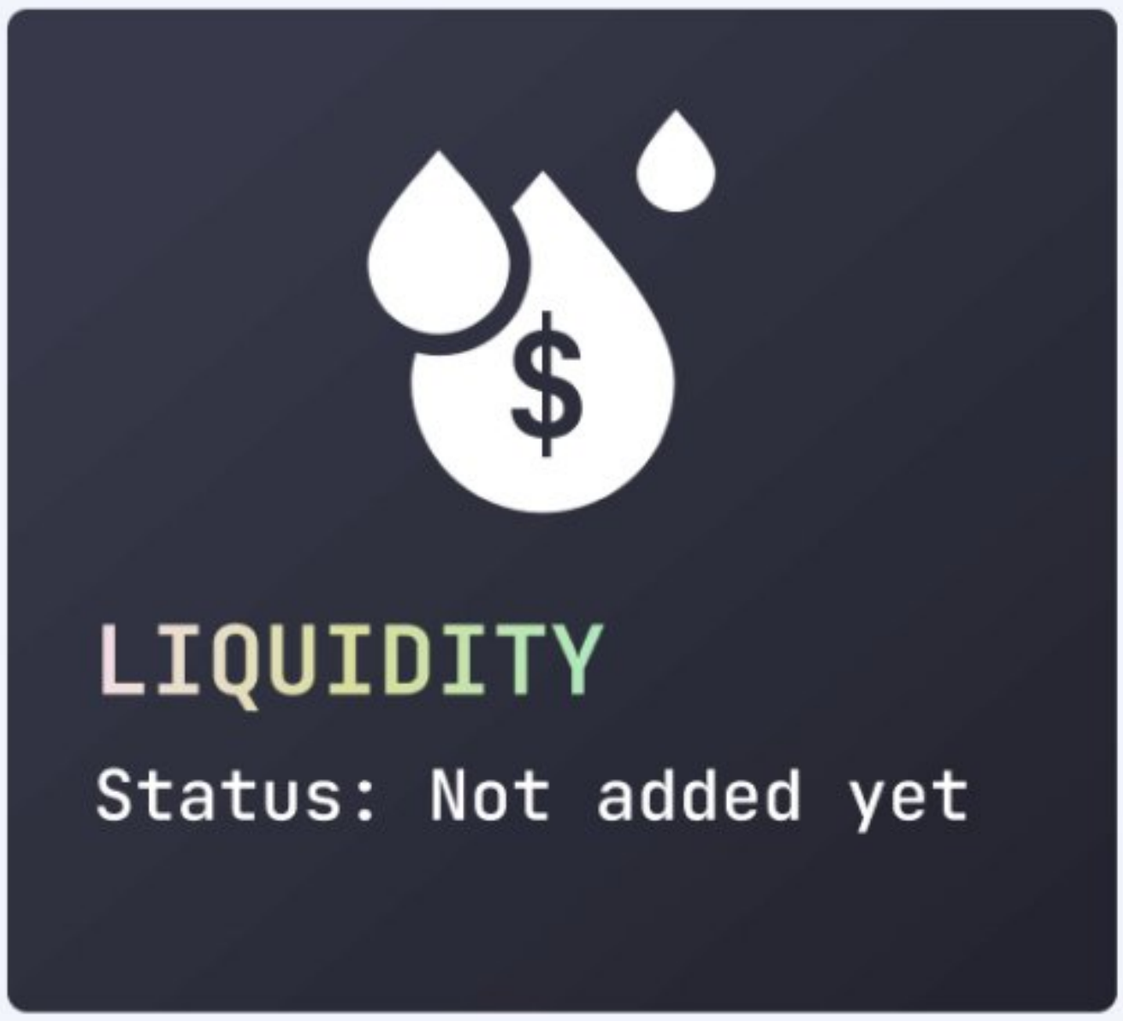
PROJECT TECHNICAL INFORMATION

(AS OF JULY 13rd, 2022)

STATUS:

HAVEN'T LAUNCHED YET

Owner Address	0xf516d22eca3220f99fd236aaac4bad9b0ca8f3ac



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

DAudit

IMPORTANT STATS

TAX	OWNER CAN SET FEES
Owner can’t set taxes	Owner can’t set fees

MAX TX AMOUNT	OWNERSHIP
Owner can't set max tx amount	Owner can renounce or transfer ownership

MINT FUNCTION	PAUSE
Owner can mint unlimited tokens.	Owner can’t pause trading

BLACKLIST	WHITELIST
Owner can’t set blacklist	Owner can’t set whitelist to avoid transaction fee

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

DAudit

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

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

DAudit

VULNERABILITY CHECK

FUNCTION REVIEW

Business Logics Review Functionality Checks	Not 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

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

DAudit

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.

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

DAudit

RISK FOUND 01

CRITICAL

Owner can mint unlimited tokens.

```
function mintBloo() external onlyOwner {
    _mint(_owner, mintAmount);
}
```

```
function mint(uint256 amount) external onlyOwner returns (bool) {
  _mint(_msgSender(), amount);
  return true;
}
```

```
  require(account != address(0), "ERC20: mint to the zero address");

  _totalSupply = _totalSupply.add(amount);
  _balances[account] = _balances[account].add(amount);
  emit Transfer(address(0), account, amount);
```

Recommendation:
It is recommended to follow the whitepaper to set a maximum mint limit of 12,000,000

Token Name:	BLOO COIN
Token Ticker	BLC
Token Platform:	POLYGON
Token Standard:	ERC20
Max. Supply (Hard Cap):	12,000,000

DAudit

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

DAudit

RISK FOUND 02

MEDIUM

Anyone that the user approves can burn their tokens

```
function burn(address account, uint256 amount) external {
  _burn(account, amount);
  _approve(account, _msgSender(), _allowances[account][_msgSender()].sub(amount, "ERC20: burn amount exceeds allowance"));
}
```

Recommendation:

Users should consider carefully before performing approve function.

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

DAudit

BLOO COIN GOOD PRACTICES FOUND

1

The owner cannot pause trading

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.

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

DAudit

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 prin 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.