



Security Assessment BLOX

Vital Block Verified On March 31th, 2023

 @Vital-Block

 @VB_Audit

 info@vitalblock.org



 www.vitalblock.org



PREPARED FOR:
BLOX FINANCE



INTRODUCTION

Auditing Company	 VITAL BLOCK SECURITY
Client Project	 BLOX FINANCE
Methodology	Automated Analysis, Manual Code Review
Language	Solidity
License	MIT
Staking Address	0x44c1813846058d6e4866e4435a757844486e60b8
Staking Address	0xf435bd39fccf4dce102833b71e1894f12089f1cd
Staking Address	0x3988dd77babde1f55bd79181cf9aa17140933e73
Network	ARBITRUM CHAIN
Optimization	200 RUNS
Token Type	ERC20
Website	https://www.bloxfi.io/
Telegram	https://t.me/+MLX2UF5RFIxmTEEx
Twitter	https://twitter.com/BLOX_FI
Discord	https://discord.gg/kxtF3txsnE
Prelim Report Date	March 29, 2023
Final Report Date	March 31, 2023

  Verify the authenticity of this report on our GitHub Repo: <https://www.github.com/vital-block>

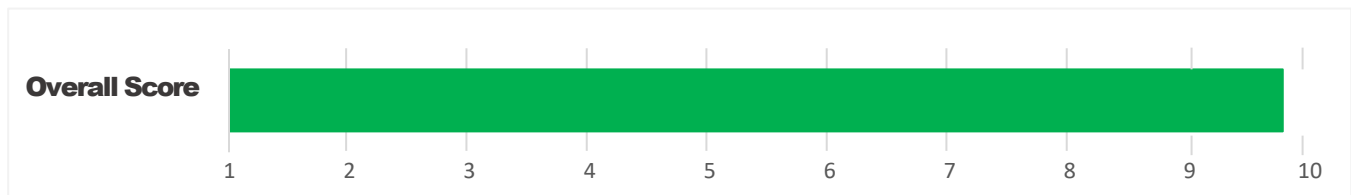


EXECUTIVE SUMMARY

Vital Block has performed the automated and manual analysis of the Sol code. The code was reviewed for common contract vulnerabilities and centralized exploits. Here's a quick audit summary:

Status	Critical ! 🔴	Major " 🟡	Medium # 🟡	Minor \$ 🟢	Unknown % 🟤
Open	0	0	0	2	0
Acknowledged	0	0	1	2	0
Resolved	0	0	0	0	0
Noteworthy OnlyOwner Privileges	Set Taxes and Ratios, Airdrop, Set Protection Settings, Set Reward Properties, Set Reflector Settings, Set Swap Settings, Set Pair and Router				

BLOX FINANCE Smart contract has achieved the following score: **99.4**



Please note that smart contracts deployed on blockchains aren't resistant to exploits, vulnerabilities and/or hacks. Blockchain and cryptography assets utilize new and emerging technologies. These technologies present a high level of ongoing risks. For a detailed understanding of risk severity, source code vulnerability, and audit limitations, kindly review the audit report thoroughly.

Please note that centralization privileges regardless of their inherited risk status - constitute an elevated impact on smart contract safety and security.



SCOPE OF WORK

Vital Block was consulted by BLOX FINANCE to conduct the smart contract audit of its .Sol source code. The audit scope of work is strictly limited to mentioned .SOL file only:

- STAKINGREWARDS.Sol

 External contracts and/or interfaces dependencies are not checked due to being out of scope.

Verify audited contract's contract address and deployed link below:

Public Staking Contract.

0x44c1813846058d6e4866e4435a757844486e60b8

0xf435bd39fccf4dce102833b71e1894f12089f1cd

0x3988dd77babde1f55bd79181cf9aa17140933e73

Contract Name	StakingRewards
Token Symbol	BLOX
Total Supply	1,000,000
Decimals	18
Blockchain	Arbitrum Network

AUDIT METHODOLOGY

Smart contract audits are conducted using a set of standards and procedures. Mutual collaboration is essential to performing an effective smart contract audit. Here's a brief overview of Vital Block auditing process and methodology:

CONNECT

- The onboarding team gathers source codes, and specifications to make sure we understand the size, and scope of the smart contract audit.

AUDIT

- Automated analysis is performed to identify common contract vulnerabilities. We may use the following third-party frameworks and dependencies to perform the automated analysis:
 - Remix IDE Developer Tool
 - Open Zeppelin Code Analyzer
 - SWC Vulnerabilities Registry
 - DEX Dependencies, e.g., Pancakeswap, Uniswap
- Simulations are performed to identify centralized exploits causing contract and/or trade locks.
- A manual line-by-line analysis is performed to identify contract issues and centralized privileges.

We may inspect below mentioned common contract vulnerabilities, and centralized exploits:

Centralized Exploits	<ul style="list-style-type: none">○ Token Supply Manipulation○ Access Control and Authorization○ Assets Manipulation○ Ownership Control○ Liquidity Access○ Stop and Pause Trading○ Ownable Library Verification
----------------------	---

Common Contract Vulnerabilities

- Integer Overflow
- Lack of Arbitrary limits
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation
- Gas Optimization
- Coding Style Violations
- Re-entrancy
- Third-Party Dependencies
- Potential Sandwich Attacks
- Irrelevant Codes
- Divide before multiply
- Conformance to Solidity Naming Guides
- Compiler Specific Warnings
- Language Specific Warnings

REPORT

- The auditing team provides a preliminary report specifying all the checks which have been performed and the findings thereof.
- The client's development team reviews the report and makes amendments to the codes.
- The auditing team provides the final comprehensive report with open and unresolved issues.

PUBLISH

- The client may use the audit report internally or disclose it publicly.






 It is important to note that there is no pass or fail in the audit, it is recommended to view the audit

as an unbiased assessment of the safety of solidity codes.



RISK CATEGORIES

Smart contracts are generally designed to hold, approve, and transfer tokens. This makes them very tempting attack targets. A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized here for the reader to review:

Risk Type	Definition
Critical ! 	These risks could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
Major " 	These risks are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to high-risk severity.
Medium # 	These risks should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution. Low-risk re-entrancy-related vulnerabilities should be fixed to deter exploits.
Minor \$ 	These risks do not pose a considerable risk to the contract or those who interact with it. They are code-style violations and deviations from standard practices. They should be highlighted and fixed nonetheless.
Unknown % 	These risks pose uncertain severity to the contract or those who interact with it. They should be fixed immediately to mitigate the risk uncertainty.

All statuses which are identified in the audit report are categorized here for the reader to review:

Status Type	Definition
Open	Risks are open.
Acknowledged	Risks are acknowledged, but not fixed.
Resolved	Risks are acknowledged and fixed.



CENTRALIZED PRIVILEGES

Centralization risk is the most common cause of cryptography asset loss. When a smart contract has a privileged role, the risk related to centralization is elevated.

There are some well-intended reasons have privileged roles, such as:

- **Privileged roles can be granted the power to `pause()` the contract in case of an external attack.**
- **Privileged roles can use functions like, `include()`, and `exclude()` to add or remove wallets from fees, swap checks, and transaction limits. This is useful to run a presale and to list on an exchange.**

Authorizing privileged roles to externally-owned-account (EOA) is dangerous. Lately, centralization-related losses are increasing in frequency and magnitude.

- **The client can lower centralization-related risks by implementing below mentioned practices:**
- **Privileged role's private key must be carefully secured to avoid any potential hack.**
- **Privileged role should be shared by multi-signature (multi-sig) wallets.**
- **Authorized privilege can be locked in a contract, user voting, or community DAO can be introduced to unlock the privilege.**
- **Renouncing the contract ownership, and privileged roles.**
- **Remove functions with elevated centralization risk.**






 **Understand the project's initial asset distribution. Assets in the liquidity pair should be locked. Assets outside the liquidity pair should be locked with a release schedule.**



Contract Ownership

0xefbdf37458e30573fee5116c97104a3a5d33c1b Is The Owner Of The Contracts.

Summary

-  Owner is not able to change or set taxes (0% tax)
-  Owner is not able to set a max amount for buys/sells/transfer
-  Owner is not able to pause trades
-  Owner is not able to mint new tokens
-  Owner is not able to blacklist an arbitrary address






Issues Found

Vital Block Security found that the **BLOX FINANCE** contracts contain no critical issue, no major issues, and 0 Major issue, in addition to 3 informational notes.

We recommend all issues are amended, while the notes are up to the team's discretion, as it refers to best practices.



AUTOMATED ANALYSIS

Symbol	Definition
	Function modifies state
	Function is payable
	Function is internal
	Function is private
	Function is important

```

**STAKINGREWARDS** | Interface | |||
| L | totalSupply | External | ! | NO |
| L | decimals | External | ! | NO |
| L | symbol | External | ! | NO |
| L | name | External | ! | NO |
| L | getOwner | External | NO |
| L | balanceOf | External | ! | NO |
| L | transfer | External | " ! ! NO |
| L | allowance | External | ! | NO |
| L | approve | External | " ! ! NO |
| L | transferFrom | External | " NO |
|||||
**IFactoryV2** | Interface | |||
| L | getPair | External | NO |
| L | createPair | External | " NO |
|||||
**IV2Pair** | Interface | |||
| L | factory | External | NO |
| L | getReserves | External | NO |
| L | sync | External | " NO |

```



|||||

| ****IRouter01**** | Interface | |||

| L | factory | External ¶ | |NO¶|

| L | ETH | External ¶ | |NO¶|

| L | addLiquidityETH | External ¶ | # |NO¶|

| L | addLiquidity | External ¶ | " |NO¶|

| L | swapExactETHForStakingRewardsTokens | External ¶ | # |NO¶|

| L | getAmountsOut | External ¶ | |NO¶|

| L | getAmountsIn | External ¶ | |NO¶|

|||||

| ****IRouter02**** | Interface | IRouter01 |||

| L | swapExactTokensForETHSupportingFeeOnStakingTokens | External ¶ | " |NO¶|

| L | swapExactETHForTokensSupportingFeeOnStakingTokens | External ¶ | # |NO¶|

| L | swapExactTokensForTokensSupportingFeeOnStakingTokens | External ¶ | " ! 🚫 |NO¶|

| L | swapExactTokensForTokens | External ¶ | " |NO¶|

|||||

| ****Protections**** | Interface | |||

| L | checkUser | External ¶ | " ! 🚫 |NO¶|

| L | setLaunch | External ¶ | " |NO¶|

| L | setLpPair | External ¶ | " |NO¶|

| L | **BLOX** | External ¶ | " |NO¶|

| L | removeSniper | External ¶ | " |NO¶|

|||||

| ****Cashier**** | Interface | |||

| L | setRewardsProperties | External ¶ | " |NO¶|

| L | tally | External ¶ | " |NO¶|

| L | load | External ¶ | # |NO¶|

| L | cashout | External ¶ | " |NO¶|

| L | giveMeWelfarePlease | External ¶ | " |NO¶|

| L | getTotalDistributed | External ¶ | |NO¶|

| L | getUserInfo | External ¶ | |NO¶|

| L | getUserRealizedRewards | External ¶ | |NO¶|



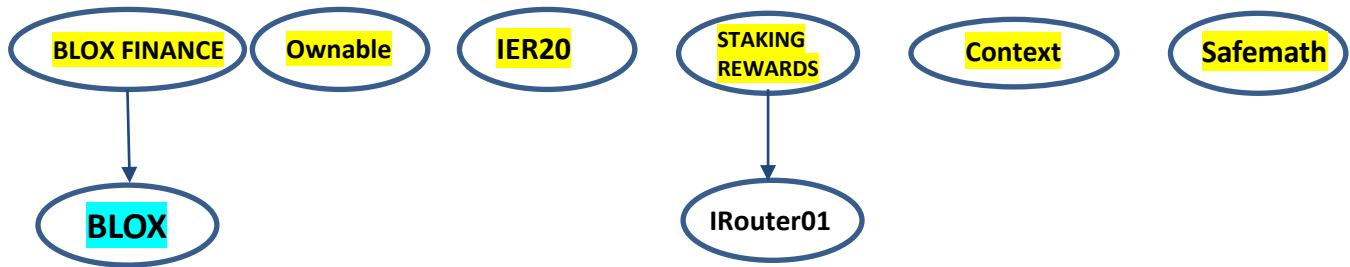
```

| L | getPendingRewards | External | | | NO |
| L | initialize | External | | " | NO |
| L | getCurrentReward | External | | | NO |
|||||
| **SOL** | Implementation | SafeMath | |||
| L | <Constructor> | Public | | # | NO |
| L | transferOwner | External | | " | onlyOwner |
| L | renounceOwnership | External | | " | NO |
| L | setOperator | Public | | " | NO |
| L | renounceOriginalDeployer | External | | " | NO |
| L | <Receive Ether> | External | | # | NO |
| L | totalSupply | External | | | NO |
| L | decimals | External | | | NO |
| L | symbol | External | | | NO |
| L | name | External | | | NO |
| L | getOwner | External | | ! | NO |
| L | balanceOf | Public | | ! | NO |
| L | allowance | External | | ! | NO |
| L | approve | External | | " ! | NO |
| L | _approve | Internal | $ | " | |
| L | approveContractContingency | Public | | " ! | onlyOwner |
| L | transfer | External | | " | NO |
| L | transferFrom | External | | " | NO |
| L | setNewRouter | External | | " | onlyOwner |
| L | setLpPair | External | | " | onlyOwner |
| L | setInitializers | External | | " | onlyOwner |
| L | isExcludedFromFees | External | | | NO |
| L | isExcludedFromDividends | External | | | NO |
| L | isExcludedFromProtection | External | | | NO |
| L | setDividendExcluded | Public | | " | onlyOwner |
| L | setExcludedFromFees | Public | | " | onlyOwner |

```



INHERITANCE GRAPH



Identifier	Definition	Severity
CEN-12	Centralization privileges of BLOX FINANCE	Medium # 🟡

Vulnerability 0 : No important security issue detected.

Threat level: Low

```

117     return
118         rewardPerTokenStored +
119         (rewardRate * (lastTimeRewardApplicable() - updatedAt) * 1e18) /
120         totalSupply;
121     }
122
123     function stake(uint _amount) external payable updateReward(msg.sender) requireNFT takeFee cooldown{
124         require(_amount > 0, "amount = 0");
125         stakingToken.transferFrom(msg.sender, address(this), _amount);
126         balanceOf[msg.sender] += _amount;
127         totalSupply += _amount;
128     }
129
130     function withdraw(uint _amount) external payable updateReward(msg.sender) requireNFT takeFee cooldown {
131         require(_amount > 0, "amount = 0");
132         balanceOf[msg.sender] -= _amount;
133         totalSupply -= _amount;
134         stakingToken.transfer(msg.sender, _amount);
135     }
136
137     function earned(address _account) public view returns (uint) {
138         return
  
```

General Detectors



Public Functions Should be Declared External

Some functions in this contract should be declared as external in order to save gas.



Attention
Required



State Variables Should be Declared Constant

Some state variables in this contract should be declared as constant



Attention
Required

- ✓ No vulnerable withdrawal functions found
- ✓ No reentrancy risk found
- ✓ No locks detected
- ✓ Verified source code found
- ✓ No mintable risks found
- ✓ Users can always transfer their tokens
- ✓ Contract cannot be upgraded
- ✓ Wallets cannot be blacklisted from transferring the token
- ✓ No transfer fees found
- ✓ Token can be sold through regular AMMs
- ✓ No transfer limits found
- ✓ No ERC20 approval vulnerability found
- ✓ Contract owner cannot abuse ERC20 approvals
- ✓ No ERC20 interface errors found
- ✓ No blocking loops found
- ✓ No centralized balance controls found
- ✓ No transfer cooldown times found
- ✓ No approval restrictions found
- ✓ No external calls detected
- ✓ No dumping risks found
- ✓ No compiler version inconsistencies found
- ✓ No unchecked call responses found
- ✓ No vulnerable self-destruct functions found
- ✓ No assertion vulnerabilities found
- ✓ No old solidity code found
- ✓ No external delegated calls found
- ✓ No external call dependency found
- ✓ No vulnerable authentication calls found
- ✓ No invalid character typos found
- ✓ No RTL characters found
- ✓ No dead code found
- ✓ No risky data allocation found
- ✓ No uninitialized state variables found
- ✓ No uninitialized storage variables found
- ✓ No vulnerable initialization functions found
- ✓ No risky data handling found
- ✓ No number accuracy bug found
- ✓ No out-of-range number vulnerability found



MANUAL REVIEW

BLOX FINANCE: BLOX FINANCE Lets Grow. Unite. Build. a permissionless ve (3,3) Dex & Liquidity market that offers 0% slippage and low costs trades , only on Arbitrum (♥, ♥)

ARBISHIELD: BLOX FINANCE

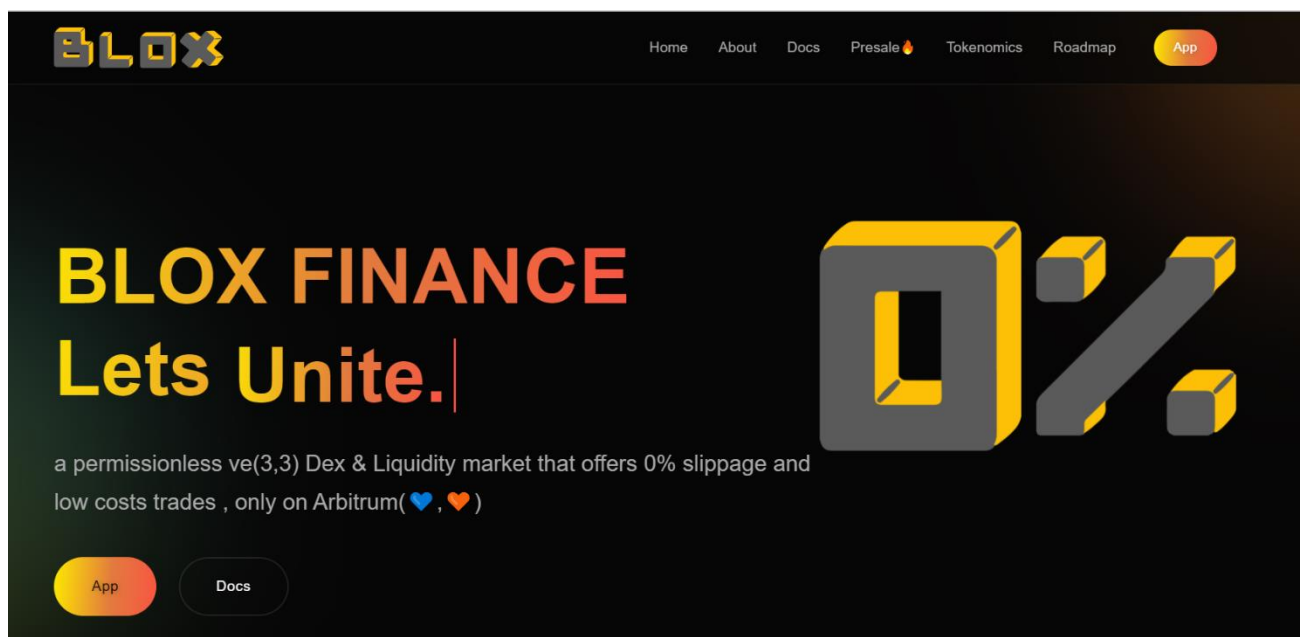
Ticker: BLOX

Decimals: 18

Chain/Standard: Arbitrum Network



Outstanding Features of BLOX Finance Launching On Arbitrum Network





ISSUES CHECKING STATUS

Issue Description

Checking Status

1.	Compiler errors.	PASSED
2.	Race Conditions and reentrancy. Cross-Function Race Conditions.	PASSED
3.	Possible Delay In Data Delivery.	PASSED
4.	Oracle calls.	PASSED
5.	Front Running.	PASSED
6.	Sol Dependency.	PASSED
7.	Integer Overflow And Underflow.	PASSED
8.	DoS with Revert.	PASSED
9.	Dos With Block Gas Limit.	PASSED
10.	Methods execution permissions.	PASSED
11.	Economy Model of the contract.	PASSED
12.	The Impact Of Exchange Rate On the solidity Logic.	PASSED
13.	Private use data leaks.	PASSED
14.	Malicious Event log.	PASSED
15.	Scoping and Declarations.	PASSED
16.	Uninitialized storage pointers.	PASSED
17.	Arithmetic accuracy.	PASSED
18.	Design Logic.	PASSED
19.	Cross-Function race Conditions	PASSED
20.	Save Upon solidity contract Implementation and Usage.	PASSED
21.	Fallback Function Security	PASSED



AUDIT RESULT

PASSED

SMART CONTRACT AUDIT OF BLOX FINANCE

Identifier	Definition	Severity
TEN-02	Staking User's Tokens	Minor 

```
function stake(uint _amount) external payable updateReward(msg.sender) requireNFT takeFee  
cooldown{  
    require(_amount > 0, "amount = 0");  
    stakingToken.transferFrom(msg.sender, address(this), _amount);  
    balanceOf[msg.sender] += _amount;  
    totalSupply += _amount;
```

Location: StakingRewards.sol#L123

Alleviation:

Any user has the authority to transfer the balance of a user's address if the user has granted allowance. The contract does not subtract the allowance in the transferFrom() method, as a result, the transfer can be repeated until the user's balance go to zero.

RECOMMENDATION

The team is advised to subtract the allowance in the transferFrom() method and migrate to a new contract..

RECOMMENDATION

Deployer and/or contract owner private keys are secured carefully.

Please refer to PAGE-09 CENTRALIZED PRIVILEGES for a detailed understanding.

ALLEVIATION

BLOX FINANCE project team understands the centralization risk. Some functions are provided privileged access to ensure a good runtime behaviour in the project



Identifier	Definition	Severity
TOB-12	Third Party Dependencies	Minor 

A smart contract is interacting with third-party protocols e.g., Uniswap, Pancakeswap router, cashier contract,

And protections contract. The scope of the audit treats third-party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and exploited. Moreover, upgrades in third parties can create severe impacts, e.g., increased transactional fees, deprecation of previous routers, etc.

RECOMMENDATION

Inspect and validate third party dependencies regularly, and mitigate severe impacts whenever necessary.



CERTIFICATE BY VITAL BLOCK SECURITY



DISCLAIMERS

Vital Block Security provides the easy-to-understand audit of Solidity, Move, and Raw source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of the code. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model, or legal compliance. This audit report does not extend to the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. Cryptographic tokens are emergent technologies, they carry high levels of technical risks and uncertainty. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without InterFi Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way



to make decisions around investment or involvement. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

FOR AVOIDANCE OF DOUBT, SERVICES, INCLUDING ANY ASSOCIATED AUDIT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

TECHNICAL DISCLAIMER

ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, VITAL BLOCK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO SERVICES, AUDIT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, VITAL BLOCK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM THE COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

WITHOUT LIMITING THE FOREGOING, VITAL BLOCK MAKES NO WARRANTY OF ANY KIND THAT ALL SERVICES, AUDIT REPORTS, SMART CONTRACT AUDITS, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET THE CLIENT’S OR ANY OTHER INDIVIDUAL’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE.

TIMELINESS OF CONTENT

The content contained in this audit report is subject to change without any prior notice. Vital Block does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following the publication.



LINKS TO OTHER WEBSITES

This audit report provides, through hypertext or other computer links, access to websites and social accounts operated by individuals other than Vital Block. Such hyperlinks are provided for your reference and convenience only and are the exclusive responsibility of such websites and social accounts owners. You agree that Vital block Security is not responsible for the content or operation of such websites and social accounts and that Vital Block shall have no liability to you or any other person or entity for the use of third-party websites and social accounts. You are solely responsible for determining the extent to which you may use any content at any other websites and social accounts to which you link from the report.



ABOUT VITAL BLOCK

Vital Block provides intelligent blockchain Security Solutions. We provide solidity and Raw Code Review, testing, and auditing services. We have Partnered with 15+ Crypto Launchpads, audited 50+ smart contracts, and analyzed 200,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Aptos, Oasis, etc.

Vital Block is Dedicated to Making Defi & Web3 A Safer Place. We are Powered by Security engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 5 core members, and 4+ casual contributors.

Website: <https://www.Vitalblock.org>

Email: info@vitalblock.org

GitHub: <https://github.com/vital-block>

Telegram (Engineering): https://t.me/vital_block

Telegram (Onboarding): https://t.me/vitalblock_cmo





vital-block



info@vitalblock.org



www.Vitalblock.org



Vital Block Dedicated to securing Public and Private Blockchain Ecosystem