SOLIDProof
Bring trust into your projects

**Blockchain Security | Smart Contract Audits | KYC Development | Marketing**

MADE IN GERMANY

# BlazeX

# AUDIT

SECURITY ASSESSMENT

## 18. July, 2023

FOR

# Introduction

SolidProof.io is a brand of the officially registered company MAKE Network GmbH, based in Germany. We're mainly focused on Blockchain Security such as Smart Contract Audits and KYC verification for project teams.
Solidproof.io assess potential security issues in the smart contracts implementations, review for potential inconsistencies between the code base and the whitepaper/documentation, and provide suggestions for improvement.

# Disclaimer

SolidProof.io reports are not, nor should be considered, an "endorsement"or "disapproval" of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

**SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.**

SolidProof.io Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. SolidProof's position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of the security or functionality of the technology we agree to analyze.

# Project Overview

## Summary

| Project Name | BlazeX |
|---|---|
| Website | https://blazex.org |
| About the project | BlazeX utilizes the full potential of the BNB Chain to deliver the wildest and most innovative tokenomics and utilities for your benefit. |
| Chain | Binance Smart Chain(BSC) |
| Language | Solidity |
| Codebase | https://bscscan.com/address/0xDD1b6B259986571A85dA82A84f461e1c212591c0#code |
| Commit | N/A |

## Social Medias

| | |
|---|---|
| Telegram | https://t.me/blazexcoin |
| Twitter | https://twitter.com/blazexcoin |
| Facebook | N/A |
| Instagram | N/A |
| GitHub | N/A |
| Reddit | N/A |
| Medium | N/A |
| Discord | N/A |
| YouTube | N/A |
| TikTok | N/A |
| LinkedIn | N/A |

## Audit Summary

| Version | Delivery Date | Change Log |
|---|---|---|
| v1.0 | 06. July 2023 | · Layout Project<br>· Automated/ Manual-Security Testing<br>· Summary |
| v1.1 | 18. July 2023 | · Reaudit |

**Note -** This Audit report consists of a security analysis of the **BlazeX** smart contract. This analysis did not include functional testing (or unit testing) of the contract's logic.

## File Overview

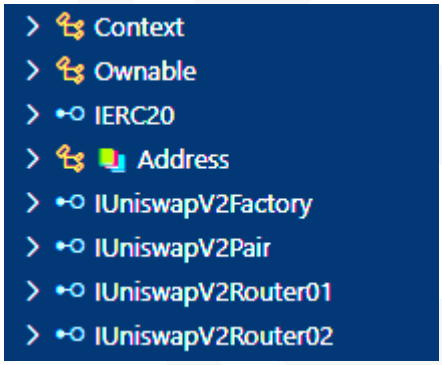
The Team provided us with the files that should be tested in the security assessment. This audit covered the following files listed below with an SHA-1 Hash.

| File Name | SHA-1 Hash |
|---|---|
| luna2.sol | d54e670b353de41c2d76f96a976e93f174164abe |

*Please note: Files with a different hash value than in this table have been modified after the security check, either intentionally or unintentionally. A different hash value may (but need not) be an indication of a changed state or potential vulnerability that was not the subject of this scan.*

## Imported Packages

*Used code from other Frameworks/Smart Contracts (direct imports).*




**Note for Investors:** We only Audited a simple reflection contract for **BlazeX**. However, If the project has other contracts (for example, a Presalecontract etc), and they were not provided to us in the audit scope, then we cannot comment on its security and are not responsible for it in any way.

# Audit Information

## Vulnerability & Risk Level

Risk represents the probability that a certain source threat will exploit the vulnerability and the impact of that event on the organization or system.The risk level is computed based on CVSS version 3.0.

| Level | Value | Vulnerability | Risk (Required Action) |
|---|---|---|---|
| **Critical** | 9 - 10 | A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken. | Immediate action to reduce risk level. |
| **High** | 7 – 8.9 | A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way. | Implementation of corrective actions as soon aspossible. |
| **Medium** | 4 – 6.9 | A vulnerability that could affect the desired outcome of executingthe contract in a specific scenario. | Implementation of corrective actions in a certain period. |
| **Low** | 2 – 3.9 | A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective. | Implementation of certain corrective actions or accepting the risk. |
| **Informational** | 0 – 1.9 | A vulnerability that have informational character but is not effecting any of the code. | An observation that does not determine a level of risk |

## Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to check the repository for security-related issues, code quality, and compliance with specifications and best practices. To this end, our team of experienced pen-testers andsmart contract developers reviewed the code line by line and documented any issues discovered.

We check every file manually. We use automated tools only so that they help us achieve faster and better results.

## Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
   a. Reviewing the specifications, sources, and instructions provided to
   SolidProof to ensure we understand the size, scope, and functionality of the
   smart contract.
   b. Manual review of the code, i.e., reading the source code line by line to identify potential vulnerabilities.
   c. Comparison to the specification, i.e., verifying that the code does what is described in the specifications, sources, and instructions provided to SolidProof.

2. Testing and automated analysis that includes the following:
   a. Test coverage analysis determines whether test cases cover code and how much code is executed when those test cases are executed.
   b. Symbolic execution, which is analysing a program to determine what inputs cause each part of a program to execute.

3. Review best practices, i.e., review smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on best practices, recommendations, and research from industry and academia.

4. Concrete, itemized and actionable recommendations to help you secure your smart contracts.

# Overall Security

## Medium or higher issues

| | |
|---|---|
| **No critical Issues found** | ✅ **Contract is safe to deploy** |
| Description | The contract does not contain issues of high or medium criticality. This means that no known vulnerabilities were found in the sourcecode. |
| Comment | N/A |

## Upgradeability

| **Contract is not an upgradable** | ✅ **Deployer cannot update the contract with new functionalities.** |
|---|---|
| Description | The contract is not an upgradeable contract. The Deployer is not able to change or add any functionalities to the contract after deploying. |
| Comment | N/A |

## Ownership

| **The ownership is not renounced** | **The owner is not renounce.** |
|---|---|
| Description | The owner has not renounced the ownership that means that the owner retains control over the contract's operations, including the ability to execute functions that may impact the contract's users or stakeholders. This can lead to several potential issues, including:<br>• Centralizations<br>• The owner has significant control over contract's operations. |
| Example | We assume that you have funds in the contract, and it has been audited by any security audit firm. Now the audit has passed. After that, the deployer can upgrade the contract to allow him to transfer the funds you purchased without any approval from you. This has the consequence that your funds can be taken by the creator. |
| Comment | N/A |

**Note** – *The contract cannot be considered as renounced till it is not deployed or having some functionality that can change the state of the contract.*

# Ownership Privileges

*These functions can be dangerous. Please note that abuse can lead to financial loss. We have a guide where you can learn more about these Functions.*

## Minting tokens

*Minting tokens refer to the process of creating new tokens in a cryptocurrency or blockchain network. This process is typically performed by the project's owner or designated authority, who has the ability to add new tokens to the network's total supply.*

| **Contract owner cannot mint new tokens** | ✅ **The owner cannot mint new tokens** |
|---|---|
| Description | The owner is not able to mint new tokens once the contract is deployed. |
| Comment | N/A |

## Burning tokens

*Burning tokens is the process of permanently destroying a certain number of tokens, reducing the total supply of a cryptocurrency or token. This is usually done to increase the value of the remaining tokens, as the reduced supply can create scarcity and potentially drive up demand.*

| **Contract owner cannot burn tokens** | ✅ **The owner cannot burn tokens** |
|---|---|
| Description | The owner is not able burn tokens without any allowances. |
| Comment | N/A |

## Blacklist addresses

*Blacklisting addresses in smart contracts is the process of adding a certain address to a blacklist, effectively preventing them from accessing or participating in certain functionalities or transactions within the contract. This can be useful in preventing fraudulent or malicious activities, such as hacking attempts or money laundering.*

| **Contract owner cannot blacklist addresses** | ✅ **The owner cannot blacklist addresses** |
|---|---|
| Description | The owner is not able blacklist addresses to lock funds. |
| Comment | N/A |

## Fees and Tax

*In some smart contracts, the owner or creator of the contract can set fees for certain actions or operations within the contract. These fees can be used to cover the cost of running the contract, such as paying for gas fees or compensating the contract's owner for their time and effort indeveloping and maintaining the contract.*

| **Contract owner cannot set fees more than 25%** | ✅ **The owner cannot set fees more than 25%.** |
|---|---|
| Description | The owner is not able to set the fees above 25%. |
| Comment | The relayer fee will be passed at the time of withdraw and it must be less than or equal to half of the denomination amount. The case is same for the Platform fee which can be set by the platform address only. |

## Lock User Funds

*In a smart contract, locking refers to the process of restricting access to certain tokens or assets for a specified period of time. When token or assets are locked in a smart contract, they cannot be transferred or used until the lock-up period has expired or certain conditions have been met.*

| **Owner cannot lock the contract** | ✅ **The owner cannot lock the contract.** |
|---|---|
| Description | The owner is not able to lock the contract by anyfunctions or updating any variables. |
| Comment | N/A |

### External/Public functions

*External/public functions are functions that can be called from outside of a contract, i.e., they can be accessed by other contracts or external accounts on the blockchain. These functions are specified using the function declaration's external or public visibility modifier.*

### State variables

*State variables are variables that are stored on the blockchain as part of the contract'sstate. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be needed within visibility modifier, such as public, private or internal, which determines the access level of the variable.*

## Components

| 📝Contracts | 📚Libraries | 🔍Interfaces | 🎨Abstract |
|---|---|---|---|
| 1 | 1 | 5 | 2 |

## Exposed Functions

*This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.*

| 🌐Public | 💰Payable |
|---|---|
| 100 | 5 |

| External | Internal | Private | Pure | View |
|---|---|---|---|---|
| 78 | 81 | 24 | 11 | 45 |

## StateVariables

| Total | 🌐Public |
|---|---|
| 41 | 18 |

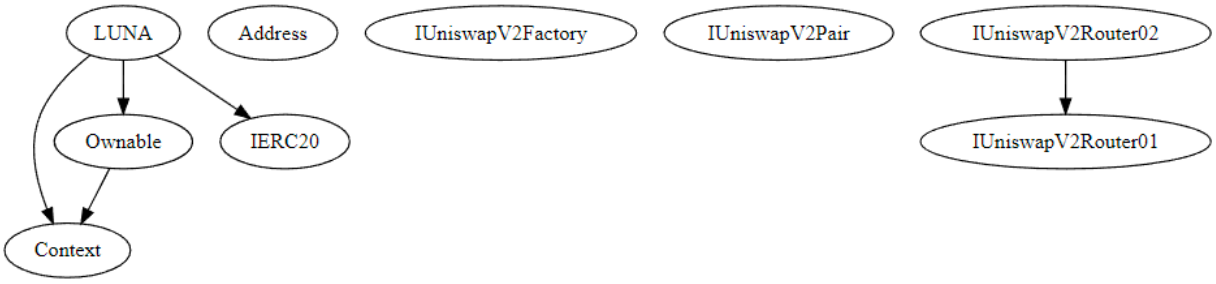
## Capabilities

| Solidity Versions observed | Experimental Features | Can Receive Funds | Uses Assembly | Has Destroyable Contracts |
|---|---|---|---|---|
| `0.8.17` | | `yes` | `yes` (2 asm blocks) | |

| Transfers ETH | Low-Level Calls | DelegateCall | Uses Hash Functions | ECRecover | New/Create/Create2 |
|---|---|---|---|---|---|
| `yes` | ------ | ---------- | ---------- | ---------- | ---------- |

## Inheritance Graph

*An inheritance graph is a graphical representation of the inheritance hierarchy among contracts. In object-oriented programming, inheritance is a mechanism that allows one class (or contract, in the case of Solidity) to inherit properties and methodsfrom another class. It shows the relationships between different contracts and how they are related to each other through inheritance.*



# Centralization Privileges

*Centralization can arise when one or more parties have privileged access or control over the contract's functionality, data, or decision-making. This can occur, for example,if the contract is controlled by a single entity or if certain participants have special permissions or abilities that others do not.*

In the project, there are authorities that have access to the following functions:

| File | Privileges |
|---|---|
| **luna2.sol** | ➢ The owner can exclude/include wallets from rewards.<br>➢ The owner can claim stuck tokens.<br>➢ The owner can enable trading only once.<br>➢ The owner can set a swap amount not less than 0.001% of the total supply.<br>➢ The owner can enable/disable swapping.<br>➢ The owner can whitelist addresses from fees.<br>➢ The owner can change the marketing wallet address.<br>➢ The owner can set buy/sell fees of not more than 10%.<br>➢ The owner can enable/disable wallet-to-wallet transfer fees.<br>➢ The owner can enable/disable the max transaction limit.<br>➢ The owner can set a max transaction amount not less than 0.1% of the total supply.<br>➢ The owner can whitelist wallets from the max transaction limit. |

## Recommendations

To avoid potential hacking risks, it is advisable for the client to manage the private key of the privileged account with care. Additionally, we recommend enhancing the security practices of centralized privileges or roles in the protocol through a decentralized mechanism or smart-contract-based accounts, such as multi-signature wallets.

Here are some suggestions of what the client can do:

- Consider using multi-signature wallets: Multi-signature wallets require multiple parties to sign off on a transaction before it can be executed, providing an extra layer of security e.g. Gnosis Safe
- Use of a timelock at least with a latency of e.g. 48-72 hours for awareness of privileged operations
- Introduce a DAO/Governance/Voting module to increase transparency and user involvement
- Consider Renouncing the ownership so that the owner cannot modify any state variables of the contract anymore. Make sure to set up everything before renouncing.

# Audit Result

## #1|Local variables shadowing (shadowing-local)

| File | Severity | Location | Status |
|---|---|---|---|
| luna2.sol | Low | L485,697, 700,701 | ACK |

### Description

- Rename the local variables that shadow another component. Changing the "owner" variable to "owner_" is recommended.

## #2| NatSpec Documentation missing

| File | Severity | Location | Status |
|---|---|---|---|
| luna2.sol | Informational | - | ACK |

### Description

- If you started to comment on your code, also comment on all other functions, variables, etc.

## #3|State variables that could be declared constant(constable-states)

| File | Severity | Location | Status |
|---|---|---|---|
| luna2.sol | Informational | L370 | ACK |

### Description

- Add the `constant` attributes to state variables that never change.

## Legend for the Issue Status

| Attribute or Symbol | Meaning |
|---|---|
| Open | The issue is not fixed by the project team. |
| Fixed | The issue is fixed by the project team. |
| Acknowledged(ACK) | The issue has been acknowledged or declared as part of business logic. |


**Blockchain Security | Smart Contract Audits | KYC Development | Marketing**

MADE IN GERMANY