



# SOLIDProof

*Bring trust into your projects*

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

MADE IN GERMANY

# IBAX Bridge

# AUDIT

**SECURITY ASSESSMENT**

**18. July, 2023**

**FOR**



**SolidProof\_io**



**@solidproof\_io**

Introduction	3
Disclaimer	3
Project Overview	4
Summary	4
Social Medias	4
Audit Summary	5
File Overview	6
Imported packages	6
Audit Information	7
Vulnerability & Risk Level	7
Auditing Strategy and Techniques Applied	8
Methodology	8
Overall Security	9
Medium or higher issues	9
Upgradeability	10
Ownership	11
Ownership Privileges	12
Minting tokens	12
Burning tokens	13
Blacklist addresses	14
Fees and Tax	15
Lock User Funds	16
Components	17
Exposed Functions	17
Capabilities	18
Inheritance Graph	19
Centralization Privileges	20
Audit Results	21



## 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	IBAX
Website	<a href="https://ibax.io/">https://ibax.io/</a>
About the project	IBAX (Integrated Blockchain Asset Exchange) is a next-generation Layer Web 3.0 blockchain infrastructure designed to be a multi-functional Swiss Army knife in the blockchain space, providing a secure, efficient, scalable, low-cost and best-in-class Baas for the ecosystem that builds on it.
Chain	IBAX Network
Language	Solidity
Codebase Link	<a href="https://github.com/IBAX-io/ibax-bridge/blob/main/contracts/Ethereum/Bridge.sol">https://github.com/IBAX-io/ibax-bridge/blob/main/contracts/Ethereum/Bridge.sol</a>
Commit	<a href="#">fddd0ec</a>
Unit Tests	Not Provided

## Social Medias

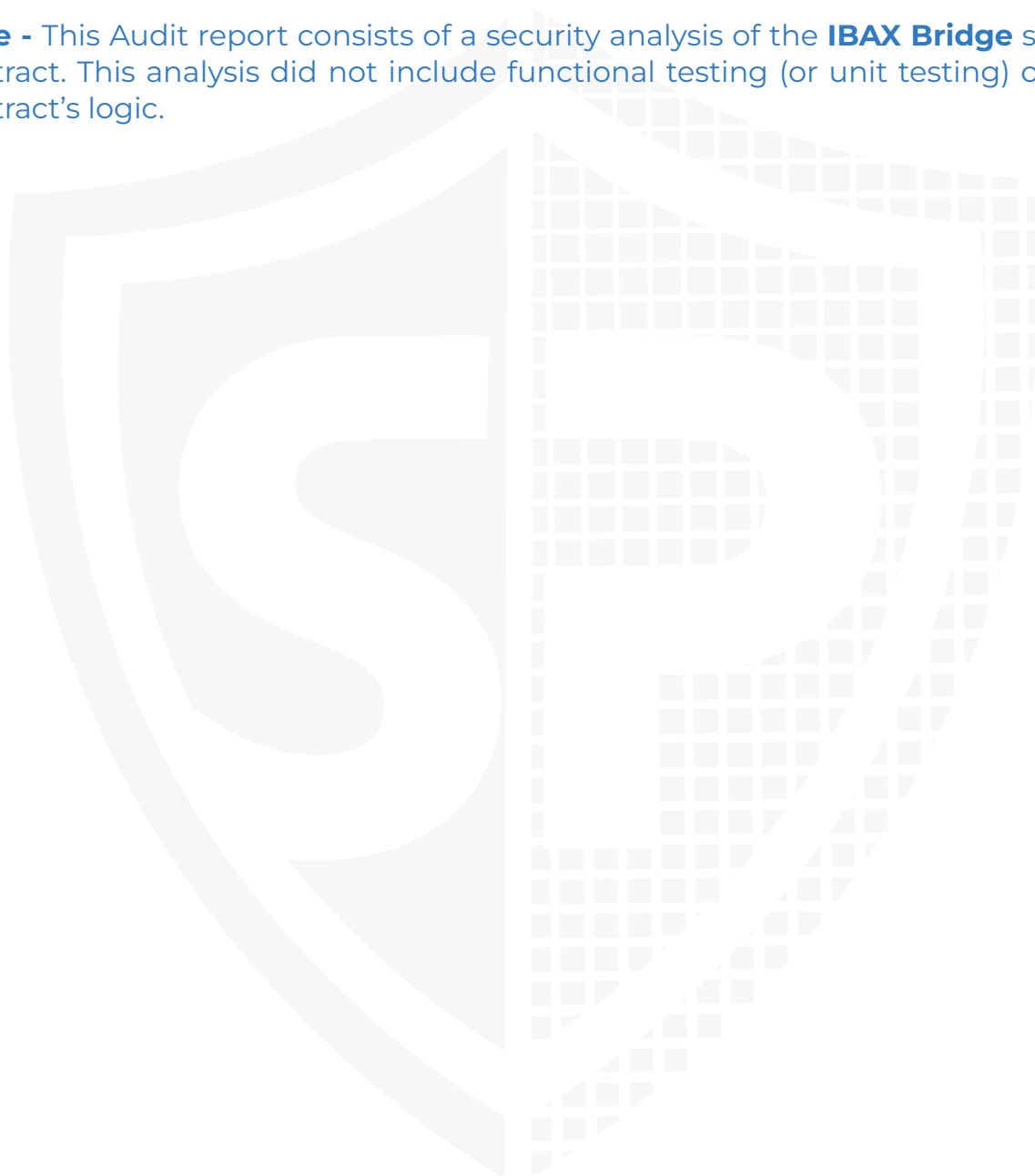
Telegram	<a href="https://t.me/IBAXNetwork">https://t.me/IBAXNetwork</a>
Twitter	<a href="https://twitter.com/IbaxNetwork">https://twitter.com/IbaxNetwork</a>
Facebook	N/A
Instagram	N/A
Github	N/A
Reddit	N/A
Medium	N/A
Discord	<a href="https://discord.gg/zRX6Mwafya">https://discord.gg/zRX6Mwafya</a>
Youtube	N/A
TikTok	N/A
LinkedIn	<a href="https://www.linkedin.com/company/68016504/admin/">https://www.linkedin.com/company/68016504/admin/</a>



## Audit Summary

Version	Delivery Date	Changelog
v1.0	18. July 2023	<ul style="list-style-type: none"> <li>• Layout Project</li> <li>• Automated- /Manual-Security Testing</li> <li>• Summary</li> </ul>

**Note** - This Audit report consists of a security analysis of the **IBAX Bridge** 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
contract/Bridge.sol	128bb9fdb39e3fca175017ad5debd431fb2b9b1e

*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).*

```
@openzeppelin/contracts/access/Ownable.sol
@openzeppelin/contracts/utils/Strings.sol
@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol
@openzeppelin/contracts/security/Pausable.sol
```

**Note for Investors:** We only Audited a bridge contract for **IBAX**. However, If the project has other contracts (for example, a Presale contract 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)
<b>Critical</b>	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.
<b>High</b>	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 as possible.
<b>Medium</b>	4 - 6.9	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.	Implementation of corrective actions in a certain period.
<b>Low</b>	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.
<b>Informational</b>	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 and smart 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

#### Critical issues found

**✗ Contract is not safe to deploy**

Description	The contract does contain issues of high or medium criticality. This means that known vulnerabilities were found in the source code and should be fixed asap.
Example	The contract is heavily centralized
Comment	N/A



## Upgradeability

**Contract is not an upgradeable**



**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:

- Centralizations
- The owner has significant control over contract's operations

Example

The owner has unanimous control over the deposit and withdrawals in the contract. Moreover, owner can also remove signer addresses, and then they won't be able to use the contract anymore.

Comment

Keep in mind that the funds can be deposited in the cotntract by anyone but in order to withdraw them, the owner has to manually add users, and only those users can withdraw.

**Note** - If the contract is not deployed, we would consider the ownership not renounced. Moreover, if there are no ownership functionalities then the ownership is automatically considered renounced.




## 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

This functionality doesn't exist in the cotntract



## 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	This functionality doesn't exist in the cotntract



## 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.

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 in developing and maintaining the contract.*

**Contract owner cannot set fees more than 25%**



**The owner cannot levy unfair taxes**

Description

The owner is not able to set the fees above 25%

Comment

There is no fees functionality in the contract.



## 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 tokens 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.*

### Contract owner can lock the user funds

**✗ The owner is able to lock the contract**

Description	Locking the contract means that the owner is able to lock any funds of addresses that they are not able to transfer bought tokens anymore.
Example	An example of locking is by pausing the contract's functionality to deposit and withdraw.
Comment	In this case it is possible for the owner to pause the withdraw function and in that case, no user will be able to withdraw their funds and they will be locked. Furthermore, the owner can remove addresses as signers and then they won't be able to withdraw.



## 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's state. They are declared at the contract level and can be accessed and modified by any function within the contract. State variables can be defined with a visibility modifier, such as public, private, or internal, which determines the access level of the variable.

## Components

 <b>Contracts</b>	 <b>Libraries</b>	 <b>Interfaces</b>	 <b>Abstract</b>
1	0	1	0


## Exposed Functions

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

 <b>Public</b>	 <b>Payable</b>
16	4




<b>External</b>	<b>Internal</b>	<b>Private</b>	<b>Pure</b>	<b>View</b>
13	9	5	6	3

## StateVariables

<b>Total</b>	 <b>Public</b>
5	5



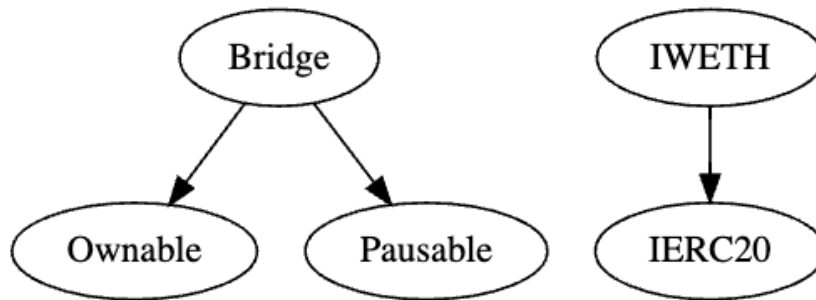
## Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
<code>^0.8.6</code>	-----	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 methods from 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
Main	<ul style="list-style-type: none"> <li>❖ <b>onlyOwner</b> <ul style="list-style-type: none"> <li>- Pause/Unpause the bridge functionalities</li> <li>- Add/Remove signer addresses</li> <li>- Update the number of signers required, but the minimum number must be greater than zero, and the maximum must be less than or equal to the signer's length.</li> </ul> </li> </ul>

## 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 Results

## #1 | Owner can lock contract

File	Severity	Location	Status
Main	Medium	L538	ACK

**Description** - The owner of the contract is able to lock the deposited tokens of the users by pausing the withdraw function. Pausing the Deposit function is okay, but we strongly recommend against the pause of the withdraw function.

## #2 | Owner can lock funds

File	Severity	Location	Status
Main	Medium	L538	ACK

**Description** - The owner of the contract is able to lock the funds of the depositors by removing them as a signer and then they won't be able to withdraw their funds. Moreover, if needed, the owner can take out those funds by setting themselves as a signer and withdrawing funds.

**Remediation** - We recommend checking the deposited balance of the signer before removing them and transferring the funds that are owed to them before removing them.

## #3 | Missing Events

File	Severity	Location	Status
Main	Low	L163—186	ACK

### Description

- Make sure to emit events for all the critical parameter changes in the contract to ensure the transparency and trackability of all the state variable changes in the contract.

## #4 | Floating Pragma

File	Severity	Location	Status
Main	Informational	L2	ACK

### Description

- The current pragma Solidity directive is "`^0.8.6`". Contracts should be deployed with the same compiler version and flag that they have

been tested thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using other versions

## #5 | NatSpec documentation missing

File	Severity	Location	Status
Main	Informational	—	ACK

### Description

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

### Legend for the Issue Status

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



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

MADE IN GERMANY