



# SOLIDProof

*Bring trust into your projects*

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

MADE IN GERMANY

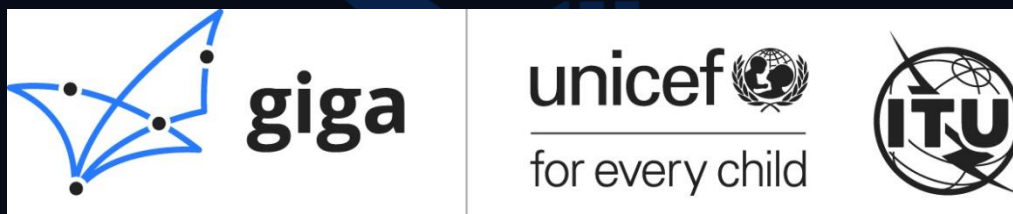
# Giga

# AUDIT

SECURITY ASSESSMENT

**31. July, 2023**

FOR





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

## 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

<b>Project Name</b>	<b>Giga</b>
<b>Website</b>	<a href="https://giga.global/">https://giga.global/</a>
<b>About the project</b>	Giga combines UNICEF's experience in education and procurement, ITU's expertise in regulation and policy, and the private sector's ability to apply tech solutions at pace. It is part of UNICEF's Office of Innovation and ITU's Telecommunication Development Bureau – two units with a track record of innovating to tackle global problems.
<b>Chain</b>	Polygon
<b>Language</b>	Solidity
<b>Codebase</b>	GigaToken: <a href="https://polygonscan.com/address/0xd8e40ccd8bcb4e5994b79a094f6f39e7a9d1b4aa#code">https://polygonscan.com/address/0xd8e40ccd8bcb4e5994b79a094f6f39e7a9d1b4aa#code</a> MultiSig: <a href="https://polygonscan.com/address/0xe1c9cdb52c9759204fda541976d15b3d6f67b546#code">https://polygonscan.com/address/0xe1c9cdb52c9759204fda541976d15b3d6f67b546#code</a> Verifier: <a href="https://polygonscan.com/address/0x8f2bec657241eb98a89012ecbe24b13be3ef8db8#code">https://polygonscan.com/address/0x8f2bec657241eb98a89012ecbe24b13be3ef8db8#code</a>
<b>Commit</b>	N/A
<b>Unit Tests</b>	Provided

## Social Medias

<b>Telegram</b>	N/A
<b>Twitter</b>	<a href="https://twitter.com/Gigaglobal">https://twitter.com/Gigaglobal</a>
<b>Facebook</b>	N/A
<b>Instagram</b>	<a href="https://www.instagram.com/giga_global/">https://www.instagram.com/giga_global/</a>
<b>GitHub</b>	N/A
<b>Reddit</b>	N/A
<b>Medium</b>	N/A
<b>Discord</b>	<a href="https://discord.com/invite/4jGNCWcVMh">https://discord.com/invite/4jGNCWcVMh</a>
<b>YouTube</b>	N/A
<b>TikTok</b>	N/A
<b>LinkedIn</b>	<a href="https://www.linkedin.com/showcase/gigaglobal/">https://www.linkedin.com/showcase/gigaglobal/</a>



## Audit Summary

Version	Delivery Date	Change Log
v1.0	06. July 2023	<ul style="list-style-type: none"> <li>· Layout Project</li> <li>· Automated/ Manual-Security Testing</li> <li>· Summary</li> </ul>
v1.1	01. August 2023	<ul style="list-style-type: none"> <li>· Reaudit</li> </ul>

**Note** - The following audit report presents a comprehensive security analysis of the smart contract utilized in the project. This analysis did not include functional testing (or unit testing) of the contract's logic. We cannot guarantee 100% logical correctness of the contract as it was not functionally tested by us.





## 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
ivttoken/contracts/interfaces/IGigaToken.sol	ad83260bd2702984754151e99594817adc6d2dfe
ivttoken/contracts/Verifier.sol	f3eeddf663c03d17a6427bedebd1c2bd88cbce51
ivttoken/contracts/Multisig.sol	43136a6c8ea7ee8726d821527a76dafde26578c4
ivttoken/contracts/GigaToken.sol	87f250721b620512ccbe724cf2a37317119f2fb5

*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.*

Dependency / Import Path	Count
@openzeppelin/contracts/access/AccessControl.sol	1
@openzeppelin/contracts/security/Pausable.sol	1
@openzeppelin/contracts/security/ReentrancyGuard.sol	1
@openzeppelin/contracts/token/ERC20/ERC20.sol	1
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol	1
@openzeppelin/contracts/token/ERC20/extensions/ERC20Snapshot.sol	1
@openzeppelin/contracts/token/ERC20/extensions/draft-ERC20Permit.sol	1
@openzeppelin/contracts/utils/cryptography/ECDSA.sol	2
@openzeppelin/contracts/utils/cryptography/draft-EIP712.sol	2

**Note for Investors:** We advise the highest caution on any presale hosted on any non-reputable launchpad website. This smart contract audit only included the mentioned file and does not support any kind of presale.





## 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 needed within 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>
3	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>
21	2





<b>External</b>	<b>Internal</b>	<b>Private</b>	<b>Pure</b>	<b>View</b>
4	21	0	0	9







## StateVariables

<b>Total</b>	 <b>Public</b>
10	10



## Capabilities

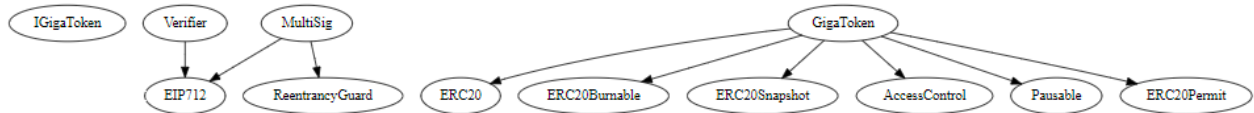
Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
<input type="text" value="^0.8.9"/> <input type="text" value="0.8.19"/> <input type="text" value="^0.8.19"/>	<input type="text" value="-----"/>	<input type="text" value="yes"/>		<input type="text" value="-----"/>

 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRrecover	 New/Create/Create2
<input type="text" value="-----"/>	<input type="text" value="-----"/>	<input type="text" value="-----"/>	<input type="text" value="Yes"/>	<input type="text" value="-----"/>	<input type="text" value="-----"/>



## 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.



## 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 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 ownership is not renounced**

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	N/A
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 can mint new tokens**

**✗ The owner can mint new tokens**

Description

Owners who have the ability to mint new tokens can reward themselves or other stakeholders, who can then sell the newly minted tokens on a cryptocurrency exchange to raise funds. However, there is a risk that the owner may abuse this power, leading to a decrease in trust and credibility in the project or platform. If stakeholders perceive that the owner is using their power to mint new tokens unfairly or without transparency, it can result in decreased demand for the token and a reduction in its value.

Comment

The minter has the ability to mint an unlimited amount of tokens.

**File, Line/s: L134 - 136**

**Codebase:**

```
function mint(address _to!, uint256 _amount!) public onlyRole(MINTER_ROLE) {
|   _mint(_to!, _amount!);
}
```



## 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 in developing 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	N/A

## 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.*

**Contract owner can lock user funds.**

**✗ The owner can lock user funds**

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.

Comment

The contract can pause the transfer of tokens by simply using pause function and after that no transfer of tokens would be possible.

**File, Line/s: L115-117**

**Codebase:**

```
function pause() public onlyRole(PAUSER_ROLE) {
|   _pause();
| }
}
```

## 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
<b>GigaToken.sol</b>	<ul style="list-style-type: none"> <li>➤ MINTER_ROLE <ul style="list-style-type: none"> <li>- Can increase/decrease unlock tokens count.</li> <li>- Can mint tokens.</li> </ul> </li> <li>➤ PAUSER_ROLE <ul style="list-style-type: none"> <li>- Can pause/unpause transfer tokens.</li> </ul> </li> <li>➤ SNAPSHOT_ROLE <ul style="list-style-type: none"> <li>- Can take snapshot of the balance and total supply.</li> </ul> </li> </ul>
<b>Multisig.sol</b>	<ul style="list-style-type: none"> <li>➤ OnlySigner <ul style="list-style-type: none"> <li>- can add multiple signers.</li> <li>- can resign from the list of signers.</li> <li>- can execute transactions.</li> <li>- can set the signers threshold not less than 2.</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 Result

### #1|Owner can mint unlimited amount of tokens

File	Severity	Location	Status
GigaToken.sol	Medium	L134-136	Open

**Description** - The owner has the ability to mint unlimited amount of tokens which can manipulate the demand and supply of the token.

### #2| Owner can pause transferring tokens

File	Severity	Location	Status
GigaToken.sol	Medium	L115-117	Open

**Description** - The contract contains the pausable functionality which can pause the transfer of tokens which results the lock of tokens and no user will be able to transfer the tokens.

### #3|Floating Pragma Solidity Version

File	Severity	Location	Status
GigaToken.sol IGigaToken.sol	Low	L2	Open

**Description** - It is recommended to add the constant version of solidity as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

### #4|Missing Arithmetic events

File	Severity	Location	Status
GigaToken.sol	Low	-	Open

**Description** - It is recommended to emit all arithmetic parameters changes.



## 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