



SOLIDProof
Bring trust into your projects

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

MADE IN GERMANY

Ridotto Lottery

Audit

**Security Assessment
28. February, 2023**

For



RIDOTTO



SolidProof_io



@solidproof_io

Disclaimer	3
Description	5
Project Engagement	5
Logo	5
Contract Link	5
Methodology	7
Used Code from other Frameworks/Smart Contracts (direct imports)	8
Tested Contract Files	9
Source Lines	10
Risk Level	10
Capabilities	11
Inheritance Graph	12
CallGraph	13
Scope of Work/Verify Claims	14
Modifiers and public functions	22
Source Units in Scope	24
Critical issues	25
High issues	25
Medium issues	25
Low issues	25
Informational issues	26
Audit Comments	26
SWC Attacks	27

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 Uniswap, 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 security or functionality of the technology we agree to analyze.

Version	Date	Description
1.0	27. February 2023	<ul style="list-style-type: none">• Layout project• Automated- /Manual-Security Testing• Summary

Network

Ethereum

Website

<https://ridotto.io>

Telegram

https://t.me/ridotto_community

Twitter

https://twitter.com/ridotto_io

Discord

<https://discord.gg/ridotto.io>



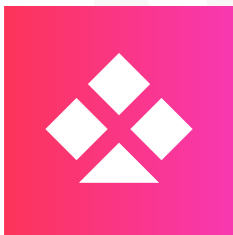
Description

Ridotto is the first cross-chain gambling and lottery protocol based on complete transparency, anonymity, security, and fairness. Our approach is to provide an open protocol, driven by the community, where users can play or build games and earn rewards by providing liquidity to the DeFi ecosystem. On top of the protocol, we developed the Ridotto platform. An easy-to-use and user-friendly app that offers a genuine and vibrant gambling experience.

Project Engagement

During the Date of 27 February 2023, **Ridotto Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

Logo



Contract Link v1.0

- Provided as Files from the following link:
 - <https://drive.google.com/file/d/1LGJ5Q6I8-Zjhm9e4AREEDarhAhKQyiNy/view>

Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. 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 as possible.
Medium	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.
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 evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
 - i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
 - ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.
2. Testing and automated analysis that includes the following:
 - i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
 - ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:

Dependency / Import Path	Count
@chainlink/contracts/src/v0.8/interfaces/VRFCoordinatorV2Interface.sol	1
@openzeppelin/contracts-upgradeable/access/AccessControlUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	2
@openzeppelin/contracts-upgradeable/security/PausableUpgradeable.sol	2
@openzeppelin/contracts-upgradeable/security/ReentrancyGuardUpgradeable.sol	1
@openzeppelin/contracts/token/ERC20/IERC20.sol	1
@openzeppelin/contracts/utils/math/Math.sol	1
@ridotto-io/global-rng/contracts/interfaces/IGlobalRng.sol	1

Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

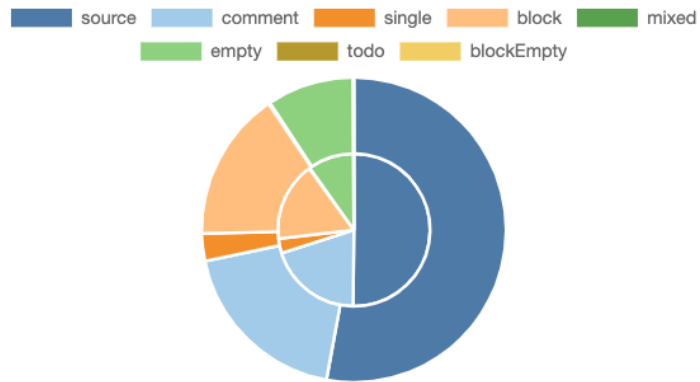
A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.

v1.0

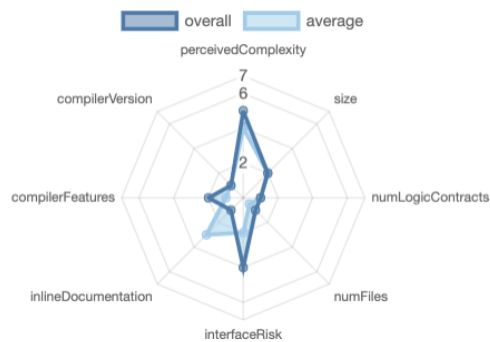
File Name	SHA-1 Hash
contracts/ RidottoLottery.sol	6ccab687a2546d082a7ec796c3beb925c93 0fbbb
contracts/GlobalRng.sol	4a4d21e1ece7d61507bf0aaef6ee133c0df73 2f4

Metrics

Source Lines v1.0



Risk Level v1.0





Capabilities

Components

 Contracts	 Libraries	 Interfaces	 Abstract
2	0	0	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.





 Public	 Payable
38	0







External	Internal	Private	Pure	View
33	37	0	2	9


StateVariables

Total	 Public
46	38

Capabilities

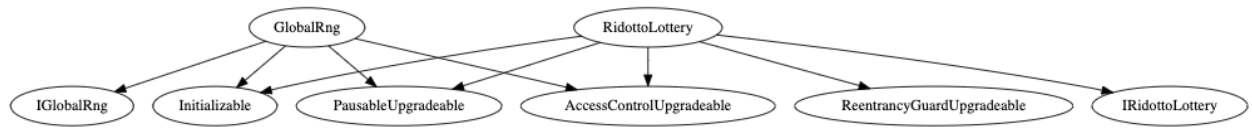
Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts
<div>^0.8.9</div>			<div>yes</div> <div>(1 asm blocks)</div>	

 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRrecover	 New/Create/Create2
<div>yes</div>			<div>yes</div>		

 TryCatch	Σ Unchecked

Inheritance Graph

v1.0



CallGraph v1.0



Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Is contract an upgradeable
2. Deployer cannot lock user funds
3. Deployer cannot pause the contract
4. Deployer cannot set fees
5. Deployer cannot blacklist/antisnipe addresses
6. Overall checkup (Smart Contract Security)



Is contract an upgradeable

Name	
Is contract an upgradeable?	Yes

Comments:

v1.0

- Owner can deploy a new version of the contract which can change any limit and give owner new privileges
 - Be aware of this and do your own research for the contract which is the contract pointing to

Write functions of the contracts v1.0

- ◆ init
- ◆ changeLotteryPeriodicity
- ◆ setLoterryMinPeriodicity
- ◆ setRngProvider
- ◆ setChainlinkCallParams
- ◆ changeIncentivePercent
- ◆ buyTickets
- ◆ buyForOthers
- ◆ setMaxBuyForOthers
- ◆ claimTickets
- ◆ closeLottery
- ◆ drawFinalNumberAndMakeLotteryClaimable
- ◆ injectFunds
- ◆ setAutoInjection
- ◆ startInitialRound
- ◆ changeLotteryParams
- ◆ startLottery
- ◆ recoverWrongTokens
- ◆ setMinAndMaxTicketPriceInLotteryToken
- ◆ setMaxNumberTicketsPerBuy
- ◆ setMaxNumberTicketsPerClaim
- ◆ setTreasuryAddress
- ◆ pause
- ◆ unPause

- ◆ init
- ◆ requestRandomWords
- ◆ <Constructor>
- ◆ rawFulfillRandomWords
- ◆ configureProvider
- ◆ addProvider

Deployer cannot burn or lock user funds

Name	Exist	Tested	Status
Deployer cannot lock	✓	✓	✗

Comments:

v1.0

- Owner can lock user funds by pausing the claim



Deployer cannot pause the contract

Name	Exist	Tested	Status
Deployer cannot pause	✓	✓	✗

Comments:

v1.0

- Owner can pause contract and stop users from claiming tickets



Deployer cannot set fees

Name	Exist	Tested	Status
Deployer cannot set fees over 25%	—	—	—
Deployer cannot set fees to nearly 100% or to 100%	—	—	—



Deployer can blacklist/antisnipe addresses

Name	Exist	Tested	Status
Deployer cannot blacklist/antisnipe addresses	—	—	—



Overall checkup (Smart Contract Security)

Tested	Verified
✓	✓

Legend

Attribute	Symbol
Verified / Checked	✓
Partly Verified	🚩
Unverified / Not checked	✗
Not available	—

Modifiers and public functions

v1.0

RidottoLottery.sol

```
◆ init
◆ changeLotteryPeriodicity
  Ⓜ onlyRole
◆ setLoterryMinPeriodicity
  Ⓜ onlyRole
◆ setRngProvider
  Ⓜ onlyRole
◆ setChainlinkCallParams
  Ⓜ onlyRole
◆ changeIncentivePercent
  Ⓜ onlyRole
◆ buyTickets
  Ⓜ notContract
  Ⓜ nonReentrant
  Ⓜ whenNotPaused
◆ buyForOthers
  Ⓜ notContract
  Ⓜ nonReentrant
  Ⓜ whenNotPaused
◆ setMaxBuyForOthers
  Ⓜ onlyRole
◆ claimTickets
  Ⓜ notContract
  Ⓜ nonReentrant
  Ⓜ whenNotPaused
◆ closeLottery
  Ⓜ nonReentrant
  Ⓜ whenNotPaused
◆ drawFinalNumberAndMakeLotteryClaimable
  Ⓜ nonReentrant
  Ⓜ whenNotPaused
◆ injectFunds
  Ⓜ whenNotPaused
◆ setAutoInjection
  Ⓜ onlyRole
◆ startInitialRound
  Ⓜ onlyRole
◆ changeLotteryParams
  Ⓜ onlyRole
◆ startLottery
  Ⓜ whenNotPaused
◆ recoverWrongTokens
  Ⓜ onlyRole
◆ setMinAndMaxTicketPriceInLotteryToken
  Ⓜ onlyRole
◆ setMaxNumberTicketsPerBuy
  Ⓜ onlyRole
◆ setMaxNumberTicketsPerClaim
  Ⓜ onlyRole
◆ setTreasuryAddress
  Ⓜ onlyRole
◆ pause
  Ⓜ onlyRole
◆ unPause
  Ⓜ onlyRole
```

GlobalRng.sol

```
◆ init
  Ⓜ initializer
◆ requestRandomWords
  Ⓜ onlyRole
  Ⓜ whenNotPaused
◆ <Constructor>
◆ rawFulfillRandomWords
◆ configureProvider
  Ⓜ onlyRole
◆ addProvider
  Ⓜ onlyRole
```

Comments

The address with the OPERATOR_ROLE have the following privileges:

- [RidottoLottery.sol](#)
 - Change lottery periodicity to any arbitrary value above or equal to 1 minute because it is also possible to change minLotteryPeriodicity.
 - Set/Update RNG provider for randomisation
 - Set chainlink parameters
 - Change incentive percent but not more than the max incentive reward value
 - Set max buy ticket numbers to any arbitrary value
 - Initialise the lottery and set/update the price of the lottery tickets
 - Enable/Disable auto injection
 - Change lottery parameters after initialisation
 - Recover tokens from the contract but not the lottery tokens
 - Set minimum and maximum ticket price, to any arbitrary value
 - Set max tickets per buy and claim to any value except zero but it is possible to set it very close to zero, for example 1,2, etc.
 - Set treasury address.
- [GlobalRng.sol](#)
 - Add and configure new chainlink provider for randomisation.
- There are several authorities which are authorized to call some functions, that means, if the owner is renounced, another address is still authorized to call functions
 - Be aware of this

Please check if an OnlyOwner or similar restrictive modifier has been forgotten.

Source Units in Scope

v1.0

File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score
contracts/RidottoLottery.sol	1	=====	1352	1252	797	306	463
contracts/GlobalRng.sol	1	=====	167	164	95	48	99
Totals	2	=====	1519	1416	892	354	562

Legend

Attribute	Description
Lines	total lines of the source unit
nLines	normalised lines of the source unit (e.g. normalises functions spanning multiple lines)
nSLOC	normalised source lines of code (only source-code lines; no comments, no blank lines)
Comment Lines	lines containing single or block comments
Complexity Score	a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Audit Results

Critical issues

No critical issues

High issues

No high issues

Medium issues

Issue	File	Type	Line	Description
#1	RidottoLottery.sol	Access Control	557	Any arbitrary user can call the close lottery function if the lottery is open and the end time is over. This will allow any user to get incentive even without being the part of lottery in the first place However, this is only possible once.
#2	RidottoLottery.sol	Weak Randomisation	319	We recommend to user off chain randomisation for the ticket numbers because on chain randomisation can be predicted.

Low issues

Issue	File	Type	Line	Description
#1	All	A floating pragma is set	—	The current pragma Solidity directive is „^0.8.9“.
#2	Ridotto Lottery.sol	Missing Events Arithmetic	1041, 1058	Emit an event for critical parameter changes
#3	Ridotto Lottery.sol	Unused State Variable	63	Make sure to remove all the unused variables. Please double check to ensure that the implementation is not forgotten.

Informational issues

Issue	File	Type	Line	Description
#1	GlobalRng.sol	Unused return values	54	Ensure that all the return values of the function calls are used and handle both success and failure cases if needed by the business logic

Audit Comments

We recommend you to use the special form of comments (NatSpec Format, Follow link for more information <https://docs.soliditylang.org/en/latest/natspec-format.html>) for your contracts to provide rich documentation for functions, return variables and more. This helps investors to make clear what that variables, functions etc. do.

28. February 2023:

- There is still an owner (Owner still has not renounced ownership)
- Owner can deploy a new version of the contract which can change any limit and give owner new privileges
- Read whole report and modifiers section for more information

SWC Attacks

ID	Title	Relationships	Status
SW C-1 36	Unencrypted Private Data On-Chain	CWE-767: Access to Critical Private Variable via Public Method	PASSED
SW C-1 35	Code With No Effects	CWE-1164: Irrelevant Code	PASSED
SW C-1 34	Message call with hardcoded gas amount	CWE-655: Improper Initialization	PASSED
SW C-1 33	Hash Collisions With Multiple Variable Length Arguments	CWE-294: Authentication Bypass by Capture-replay	PASSED
SW C-1 32	Unexpected Ether balance	CWE-667: Improper Locking	PASSED
SW C-1 31	Presence of unused variables	CWE-1164: Irrelevant Code	PASSED
SW C-1 30	Right-To-Left-Override control character (U+202E)	CWE-451: User Interface (UI) Misrepresentation of Critical Information	PASSED
SW C-1 29	Typographical Error	CWE-480: Use of Incorrect Operator	PASSED
SW C-1 28	DoS With Block Gas Limit	CWE-400: Uncontrolled Resource Consumption	PASSED

SW C-1 27	Arbitrary Jump with Function Type Variable	CWE-695: Use of Low-Level Functionality	PASSED
SW C-1 25	Incorrect Inheritance Order	CWE-696: Incorrect Behavior Order	PASSED
SW C-1 24	Write to Arbitrary Storage Location	CWE-123: Write-what-where Condition	PASSED
SW C-1 23	Requirement Violation	CWE-573: Improper Following of Specification by Caller	PASSED
SW C-1 22	Lack of Proper Signature Verification	CWE-345: Insufficient Verification of Data Authenticity	PASSED
SW C-1 21	Missing Protection against Signature Replay Attacks	CWE-347: Improper Verification of Cryptographic Signature	PASSED
SW C-1 20	Weak Sources of Randomness from Chain Attributes	CWE-330: Use of Insufficiently Random Values	PASSED
SW C-11 9	Shadowing State Variables	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-11 8	Incorrect Constructor Name	CWE-665: Improper Initialization	PASSED
SW C-11 7	Signature Malleability	CWE-347: Improper Verification of Cryptographic Signature	PASSED

SW C-11 6	Timestamp Dependence	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 5	Authorization through tx.origin	CWE-477: Use of Obsolete Function	PASSED
SW C-11 4	Transaction Order Dependence	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	PASSED
SW C-11 3	DoS with Failed Call	CWE-703: Improper Check or Handling of Exceptional Conditions	PASSED
SW C-11 2	Delegatecall to Untrusted Callee	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	PASSED
SW C-11 1	Use of Deprecated Solidity Functions	CWE-477: Use of Obsolete Function	PASSED
SW C-11 0	Assert Violation	CWE-670: Always-Incorrect Control Flow Implementation	PASSED
SW C-1 09	Uninitialized Storage Pointer	CWE-824: Access of Uninitialized Pointer	PASSED
SW C-1 08	State Variable Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED
SW C-1 07	Reentrancy	CWE-841: Improper Enforcement of Behavioral Workflow	PASSED
SW C-1 06	Unprotected SELFDESTRUCT Instruction	CWE-284: Improper Access Control	PASSED

SW C-1 05	Unprotected Ether Withdrawal	CWE-284: Improper Access Control	PASSED
SW C-1 04	Unchecked Call Return Value	CWE-252: Unchecked Return Value	PASSED
SW C-1 03	Floating Pragma	CWE-664: Improper Control of a Resource Through its Lifetime	NOT PASSED
SW C-1 02	Outdated Compiler Version	CWE-937: Using Components with Known Vulnerabilities	PASSED
SW C-1 01	Integer Overflow and Underflow	CWE-682: Incorrect Calculation	PASSED
SW C-1 00	Function Default Visibility	CWE-710: Improper Adherence to Coding Standards	PASSED

*Solid
Proofed*

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


MADE IN GERMANY