CERTIK

Code Security Assessment

iSwap VI-1

Jan 26th, 2022

Table of Contents

Summary

This report has been prepared for iSwap VI-1 to discover issues and vulnerabilities in the source code of the iSwap VI-1 project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	iSwap VI-1
Platform	other
Language	Solidity
Codebase	https://github.com/dappiswap/iswap-contract
Commit	65e07ded9f18c53460ba2279f8fac05e433091f8

Audit Summary

Delivery Date	Jan 26, 2022
Audit Methodology	Static Analysis, Manual Review

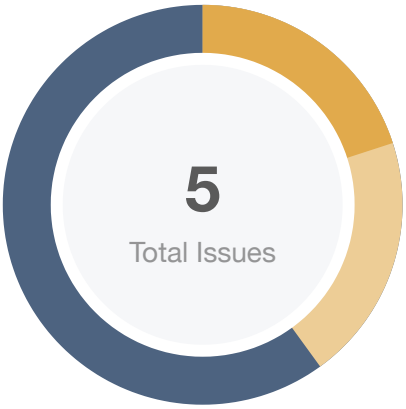
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Mitigated	Resolved
Critical	0	0	0	0	0	0	0
Major	0	0	0	0	0	0	0
Medium	1	0	0	1	0	0	0
Minor	1	0	0	0	0	0	1
Informational	3	0	0	2	0	0	1
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
ISA	ISwapArbitrumBridge.sol	057056bffc36a69e98b273f1d2af9f3135d12d367a32edcf2e1c836848cc687f
ISB	ISwapAvaxBridge.sol	483e5e2ababe105afafa756d8cb306ab976e6b7b2f3e68abf79ef19ab8e528c0
ISI	ISwapBaseBridge.sol	156e15475961d108052462ebed65eab6c8eda766a37bf6f08b71333f5967b052
ISO	ISwapBaseBridgeOptimization.sol	5e114034448de94c1a4069aab807718d5627a357af020be8852107cffdc0af5b
ISS	ISwapBaseStorage.sol	80444eae611c88fe770f654d635b23f66cf71da8630862bd3aa6f69dfbec0562
ISC	ISwapBscBridge.sol	fd9ad309b1dd277d20f390e62e74316a73e9af7827e4e9dcdeabad6e7c2ad6ec
ISE	ISwapEthBridge.sol	07823469defeecbf5d1f68d74192ccde3f14d074ec5f89c29a9d1d8b7c5afa66
ISF	ISwapFtmBridge.sol	da9946749bb67932990ead349eba65fed024086b84ee824d8aa90cd5c54bcb05
ISH	ISwapHecoBridge.sol	0696dd77e54eb4d862b2ac52b42224d4afbcae124cbed54ca941a02438b78849
ISK	ISwapOecBridge.sol	adad2c13d4ead6b99913f11e415a9e942dde9a168362b3a7970895fe9376b8f5
ISP	ISwapPolygonBridge.sol	1a0c35db1d6e900602497cd9fa7eaef22bbdb14fc949a9577cff377d920c0c25

Findings



Critical	**0** (0.00%)
Major	**0** (0.00%)
Medium	**1** (20.00%)
Minor	**1** (20.00%)
Informational	**3** (60.00%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
iSwap-01	Financial Models	Logical Issue	Minor	Resolved
ISC-01	Third Party Dependencies	Volatile Code	Informational	Resolved
ISI-01	Centralization Related Risks	**Centralization / Privilege**	**Medium**	Acknowledged
ISI-02	Unlocked compiler version	Language Specific	Informational	Acknowledged
ISI-03	Improper usage of `public` and `external` type	Gas Optimization	Informational	Acknowledged

iSwap-01 | Financial Models

Category	Severity	Location	Status
Logical Issue	Minor	Global	Resolved

Description

The `ISwap` protocol mainly provides functions as follows:

1. **Normal Swap**: Users can swap one kind of token to another token in the same chain.
2. **Cross-chain Swap**: Users can swap one kind of token in one chain to another token in the other chain.
3. **Optimized Normal Swap**: The protocol provides an optimized swap plan. The contract will swap tokens in different DEX protocols to maximize the number of token users swapped out.

And then, there are some questions.

1. The parameter `amount` in the function `refund()` is specified by the function caller. How does our system make the `amount` is as many as the real amount that belongs to the users?
2. There are two steps to `Cross-chain Swap`. 1. The contract will swap the user's token to the bridge token in the source chain and emit events. 2. The contract in the destination chain will swap the bridge token to the token users want. How does our system make sure the data in the source chain and destination chain are the same.

Recommendation

Financial models of blockchain protocols need to be resilient to attacks. They need to pass simulations and verifications to guarantee the security of the overall protocol.

The financial model of this protocol is not in the scope of this audit.

Alleviation

[iSwap]:

1. The refund amount is controlled by the centralized program, which will deduct gas consumption from the token paid by the user, and then return the remaining funds to the user. This feature is for market makers only.
2. The centralized program will associate the source chain and target chain transactions, and users can ensure the consistency of the source chain data and the target chain data by querying the cross-

chain transaction records.

ISC-01 | Third Party Dependencies

Category	Severity	Location	Status
Volatile Code	Informational	ISwapBaseBridge.sol: 140, 186~188 ISwapBaseStorage.sol: 14~16	Resolved

Description

The contract is serving as the underlying entity to interact with some third-party protocols or tool libraries. The scope of the audit treats 3rd party entities as black boxes and assumes their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Recommendation

We understand that the business logic of `ISwapBaseBridge` and `ISwapBaseBridgeOptimization` requires interaction with some DEX protocols, some tool libraries, etc. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[iSwap]: We will pay attention when we add 3rd-party DEX and tool, their security will be checked.

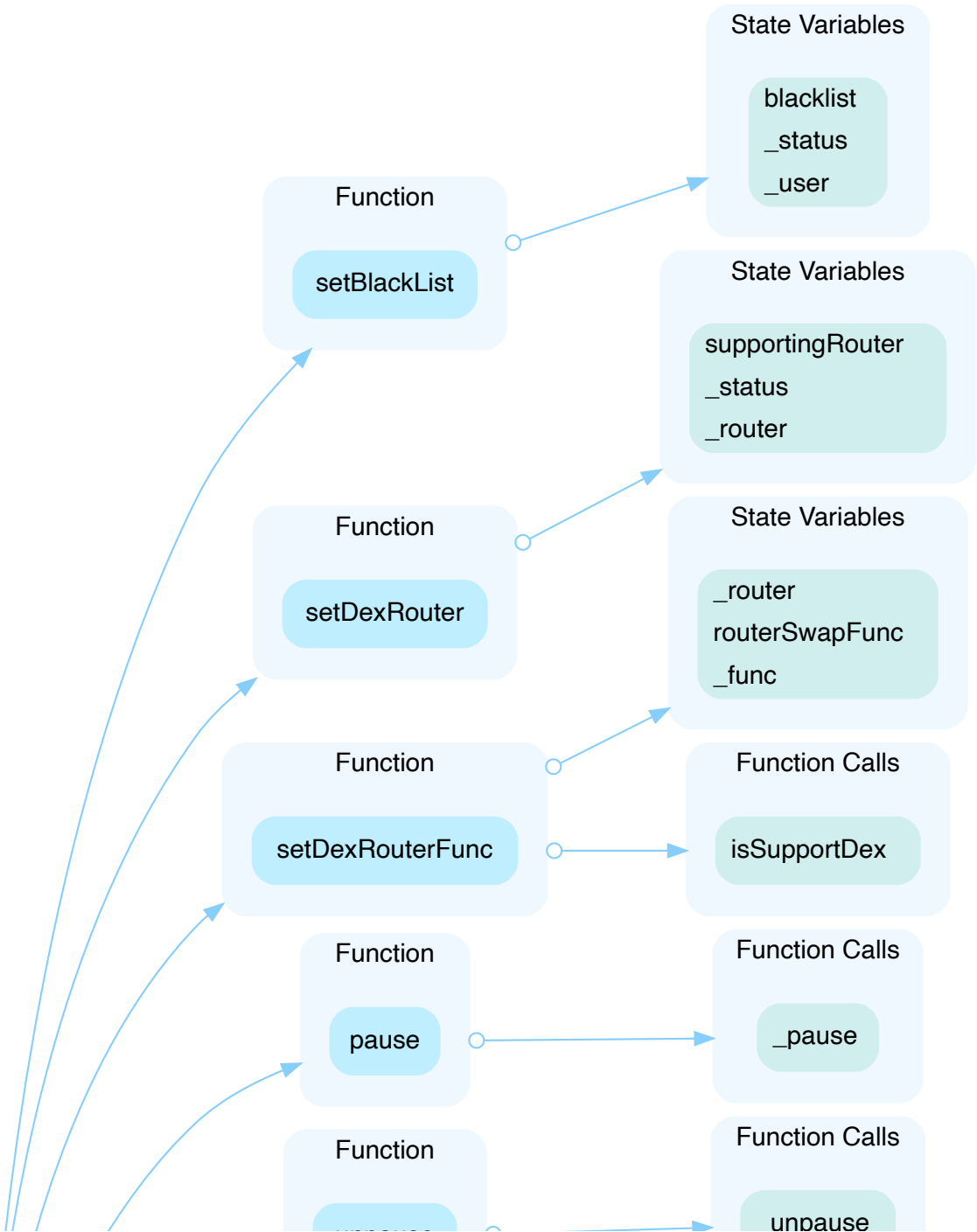
ISI-01 | Centralization Related Risks

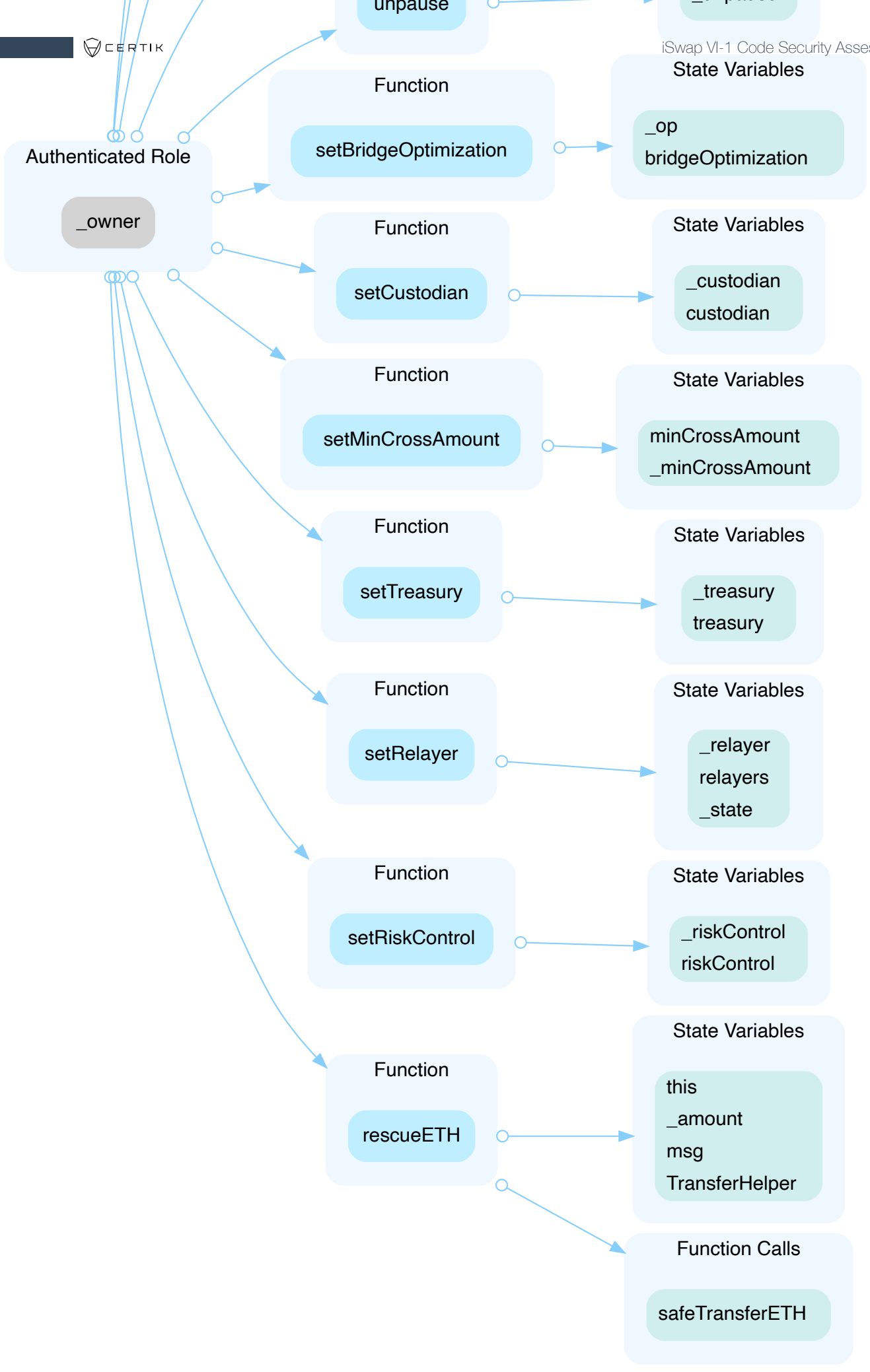
Category	Severity	Location	Status
Centralization / Privilege	Medium	ISwapBaseBridge.sol: 440~443, 447~450, 453~456, 459~461, 464~466, 469~473, 476~480, 483~486, 489~493, 496~500, 503~507, 548~556, 511~526, 359~373, 376~430, 530~544	Acknowledged

Description

In the contract, `ISwapBaseBridge`, the role, `_owner`, has authority over the functions shown in the diagram below.

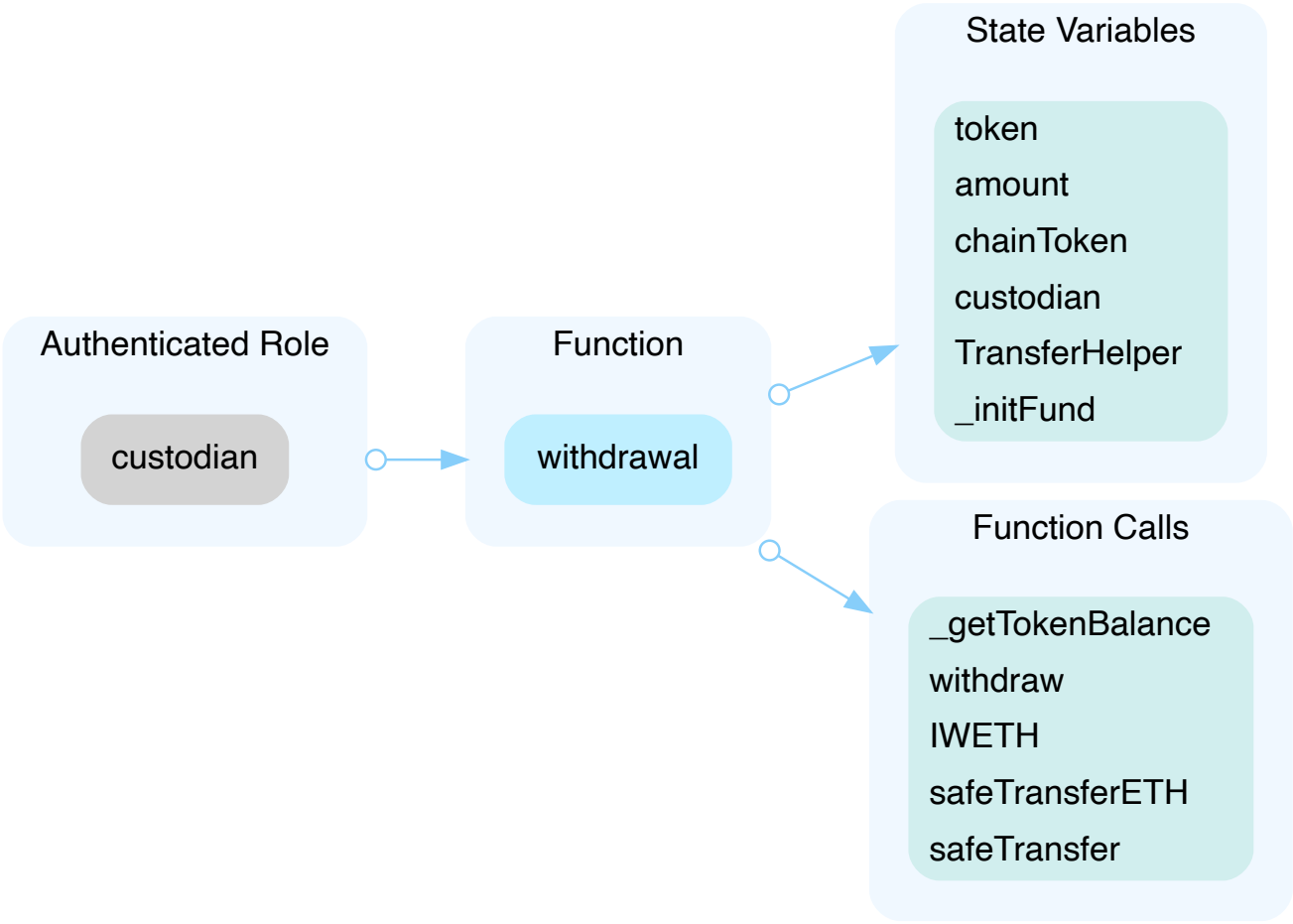
Any compromise to the `_owner` account may allow the hacker to take advantage of this authority.




unpause
Function
setBridgeOptimization
State Variables
_op
bridgeOptimization
Authenticated Role
_owner
Function
setCustodian
State Variables
_custodian
custodian
Function
setMinCrossAmount
State Variables
minCrossAmount
_minCrossAmount
Function
setTreasury
State Variables
_treasury
treasury
Function
setRelayer
State Variables
_relayer
relayers
_state
Function
setRiskControl
State Variables
_riskControl
riskControl
State Variables
this
_amount
msg
TransferHelper
Function
rescueETH
Function Calls
safeTransferETH

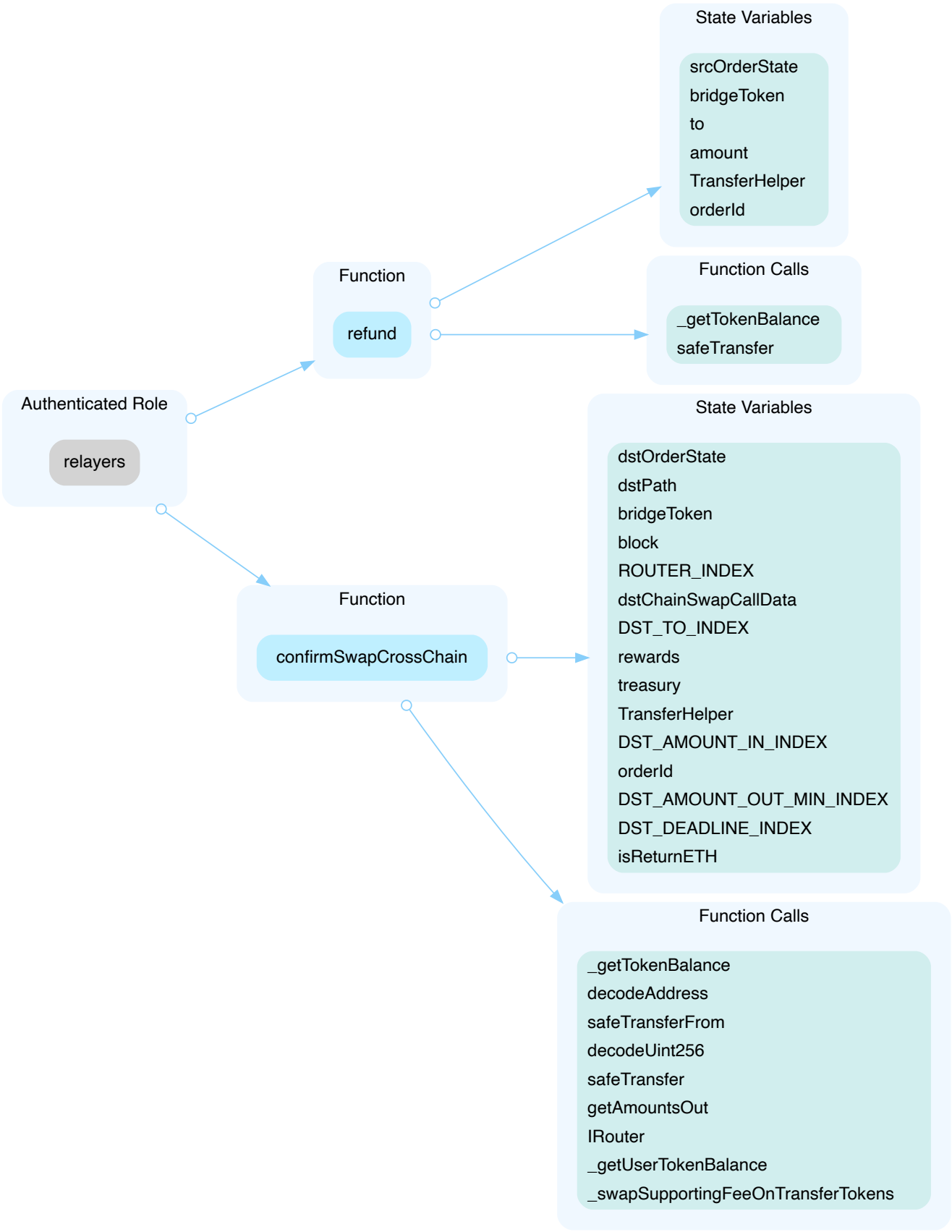
In the contract, `ISwapBaseBridge`, the role, `custodian`, has authority over the functions shown in the diagram below.

Any compromise to the `custodian` account may allow the hacker to take advantage of this authority.



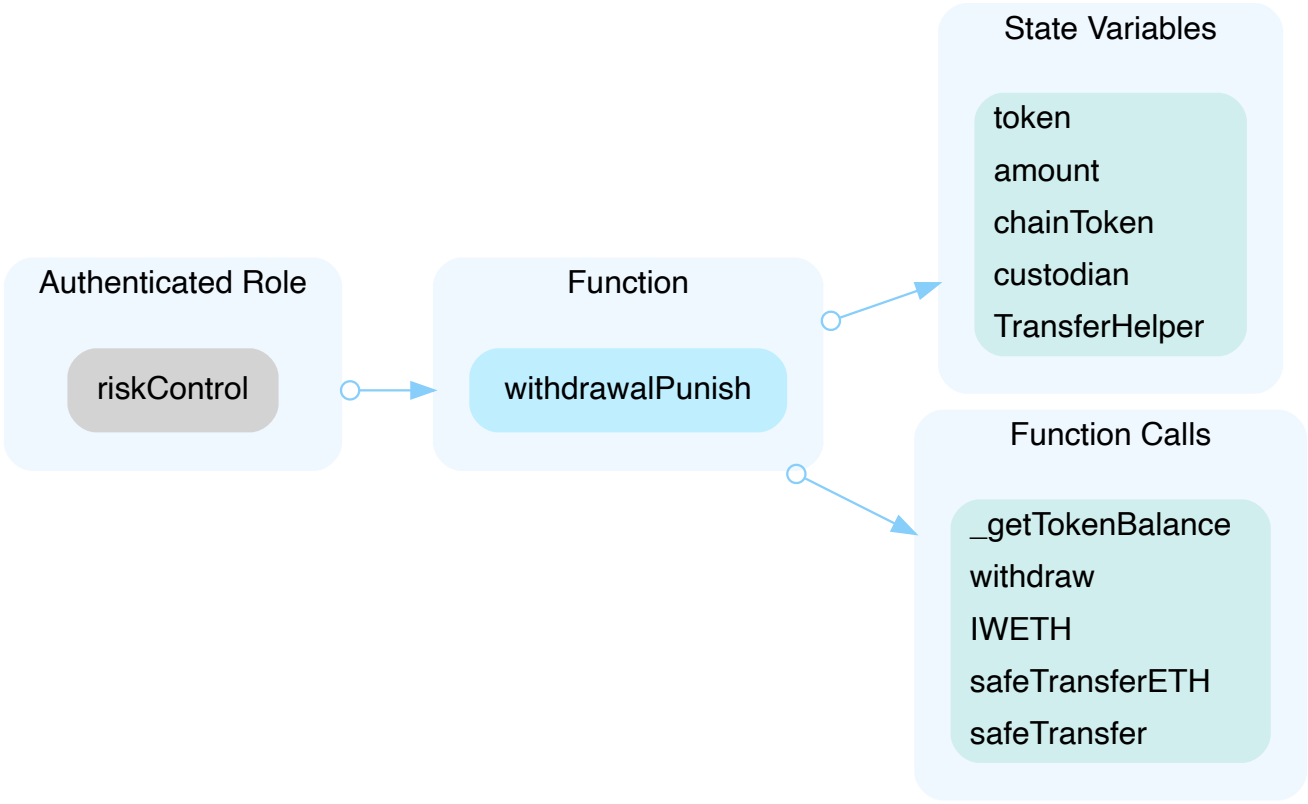
In the contract, `ISwapBaseBridge`, the role, `relayers`, has authority over the functions shown in the diagram below.

Any compromise to the `relayers` account may allow the hacker to take advantage of this authority.



In the contract, `ISwapBaseBridge`, the role, `riskControl`, has authority over the functions shown in the diagram below.

Any compromise to the `riskControl` account may allow the hacker to take advantage of this authority.



Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations; AND

- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

Alleviation

[iSwap Team]: We have a strict private key protection mechanism (signature machine mechanism), which is difficult to be attacked.

1. The private key is generated, encrypted, and stored by multiple parties. It can be accessed only after each party is authorized one by one;
2. During the signing process, we need to obtain partial private keys from multiple parties by encrypted transmission, and assemble them into the private key to complete the signature;
3. Hackers need to break the `ISwap` firewall first, then break multiple parties. Hackers need to break several symmetric and asymmetric encryption algorithms during this process, which is extremely difficult.

We have a strong emergency response mechanism:

1. We do not issue tokens and there are no user lock-ups, so user assets will not suffer losses;

2. We have a complete monitoring mechanism. When abnormal conditions such as the abnormal decrease of assets, loss of cross-chain transactions, inconsistent request hashes, etc. occur, the problem can be found within five minutes and resolved in time.

ISI-02 | Unlocked compiler version

Category	Severity	Location	Status
Language Specific	Informational	ISwapBaseBridge.sol: 2	Acknowledged

Description

The contract has unlocked compiler version. An unlocked compiler version in the source code of the contract permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to different compiler versions. This can lead to an ambiguity when debugging as compiler specific bugs may occur in the codebase that would be hard to identify over a span of multiple compiler versions rather than a specific one.

Recommendation

We advise that the compiler version is instead locked at the lowest version possible that the contract can be compiled at. For example, for version `>=0.6.0 <0.8.0` the contract should contain the following line:

```
pragma solidity 0.8.0;
```

Alleviation

iSwap team acknowledged this finding.

ISI-03 | Improper usage of `public` and `external` type

Category	Severity	Location	Status
Gas Optimization	Informational	ISwapBaseBridge.sol: 274~309	Acknowledged

Description

`public` functions that are never called by the contract could be declared as `external`. `external` functions are more efficient than `public` functions.

Recommendation

Consider using the external attribute for public functions that are never called within the contract.

Alleviation

iSwap team acknowledged this finding.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. 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. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR 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, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'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. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

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

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.