CERTIK

Security Assessment

Sperax VI

Dec 22nd, 2021

Table of Contents

Summary

This report has been prepared for Sperax VI to discover issues and vulnerabilities in the source code of the Sperax VI 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	Sperax VI
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/CertiKProject/certik-audit-contracts
Commit	bc3e015112af273ec285fb5812d99fac02e7ee35

Audit Summary

Delivery Date	Dec 22, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

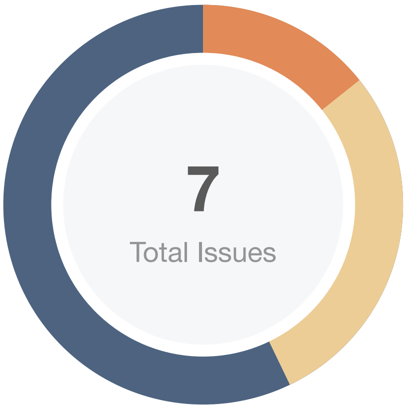
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
● Critical	0	0	0	0	0	0
● Major	1	0	0	1	0	0
● Medium	0	0	0	0	0	0
● Minor	2	0	0	2	0	0
● Informational	4	0	0	4	0	0
● Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
SPA	farm_SPA_USDs.sol	76d5f1f0a0e44b5f9beda5b053e0350edec9c545f337a6dd29f441aeea1f767d

Findings



🟥	**Critical**	**0** (0.00%)
🟧	**Major**	**1** (14.29%)
🟨	**Medium**	**0** (0.00%)
🟨	**Minor**	**2** (28.57%)
🟦	**Informational**	**4** (57.14%)
🟩	**Discussion**	**0** (0.00%)

ID	Title	Category	Severity	Status
Sperax-01	Financial Models	Logical Issue	● Informational	ⓘ Acknowledged
SPA-01	Centralization Risk	**Centralization / Privilege**	● **Major**	ⓘ Acknowledged
SPA-02	Redundant Code Components	Volatile Code	● Informational	ⓘ Acknowledged
SPA-03	Variables that could be declared as `constant`	Gas Optimization	● Informational	ⓘ Acknowledged
SPA-04	Unknown Imported Source File	Logical Issue	● Minor	ⓘ Acknowledged
SPA-05	Third Party Dependencies	Volatile Code	● Minor	ⓘ Acknowledged
SPA-06	Extensive precision conversion	Mathematical Operations	● Informational	ⓘ Acknowledged

Sperax-01 | Financial Models

Category	Severity	Location	Status
Logical Issue	● Informational	Global	ⓘ Acknowledged

Description

The main content of the current audit is: users obtain SPA rewards by staking SPA-USDs liquidity (represented as NFT in uniswapV3) on a regular or irregular basis.

It is worth noting that this financial model is not complete. For example, the creation of related pools on UniswapV3, the creation of user liquidity, and user pledge liquidity are all missing.

The callback method `_checkOnERC721Received` is a method for users to calculate rewards and bookkeeping after transferring liquidity to the current pledge contract, rather than a specific user pledge method.

This financial model is not in the scope of the audit.

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

Sperax team acknowledged this finding.

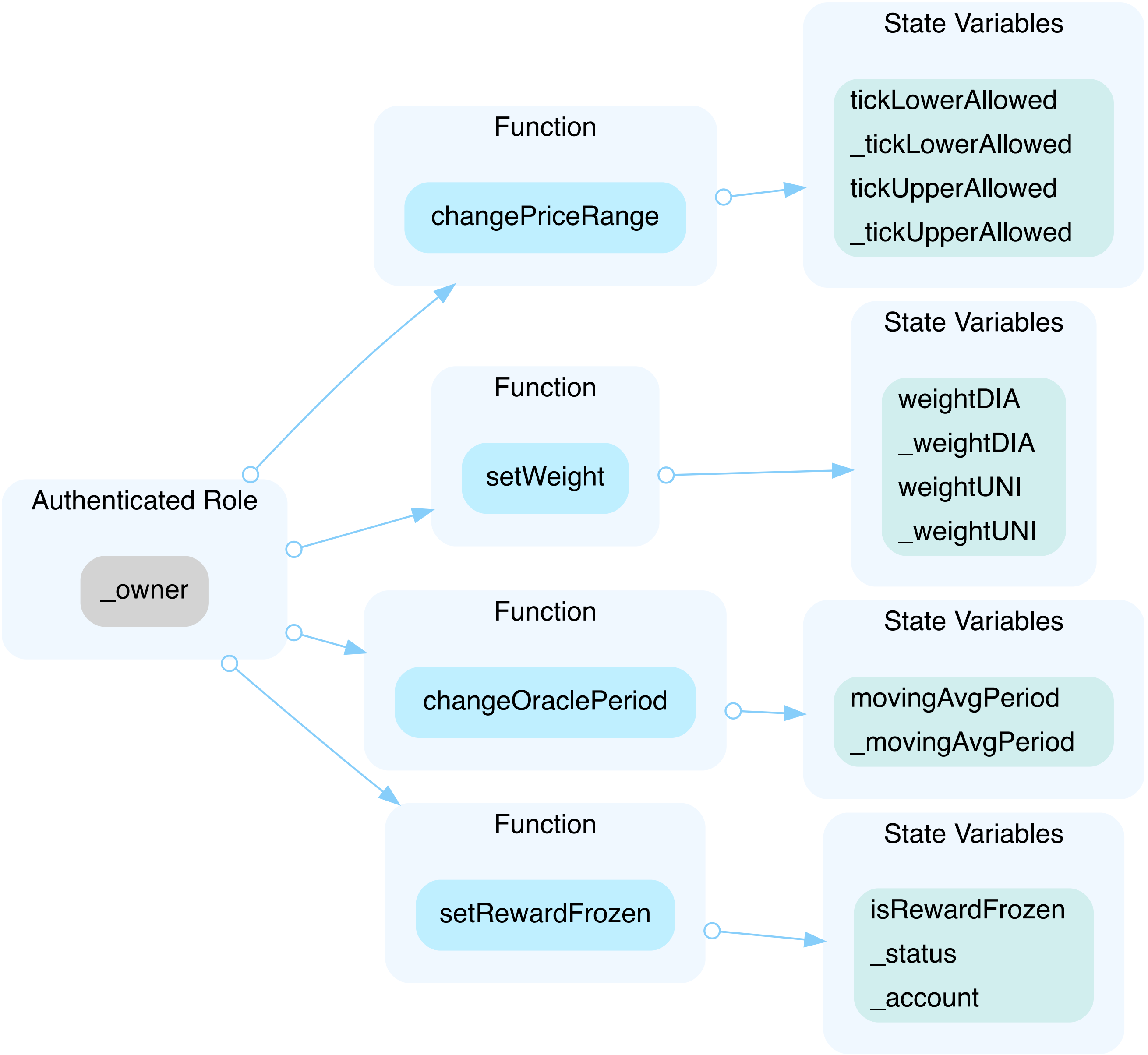
SPA-01 | Centralization Risk

Category	Severity	Location	Status
Centralization / Privilege	● Major	contract/farm_SPA_USDs.sol (fe7bde7): 468~472, 474~478, 480~483, 485~488, 294~298, 300~304, 306~309, 311~314	ⓘ Acknowledged

Description

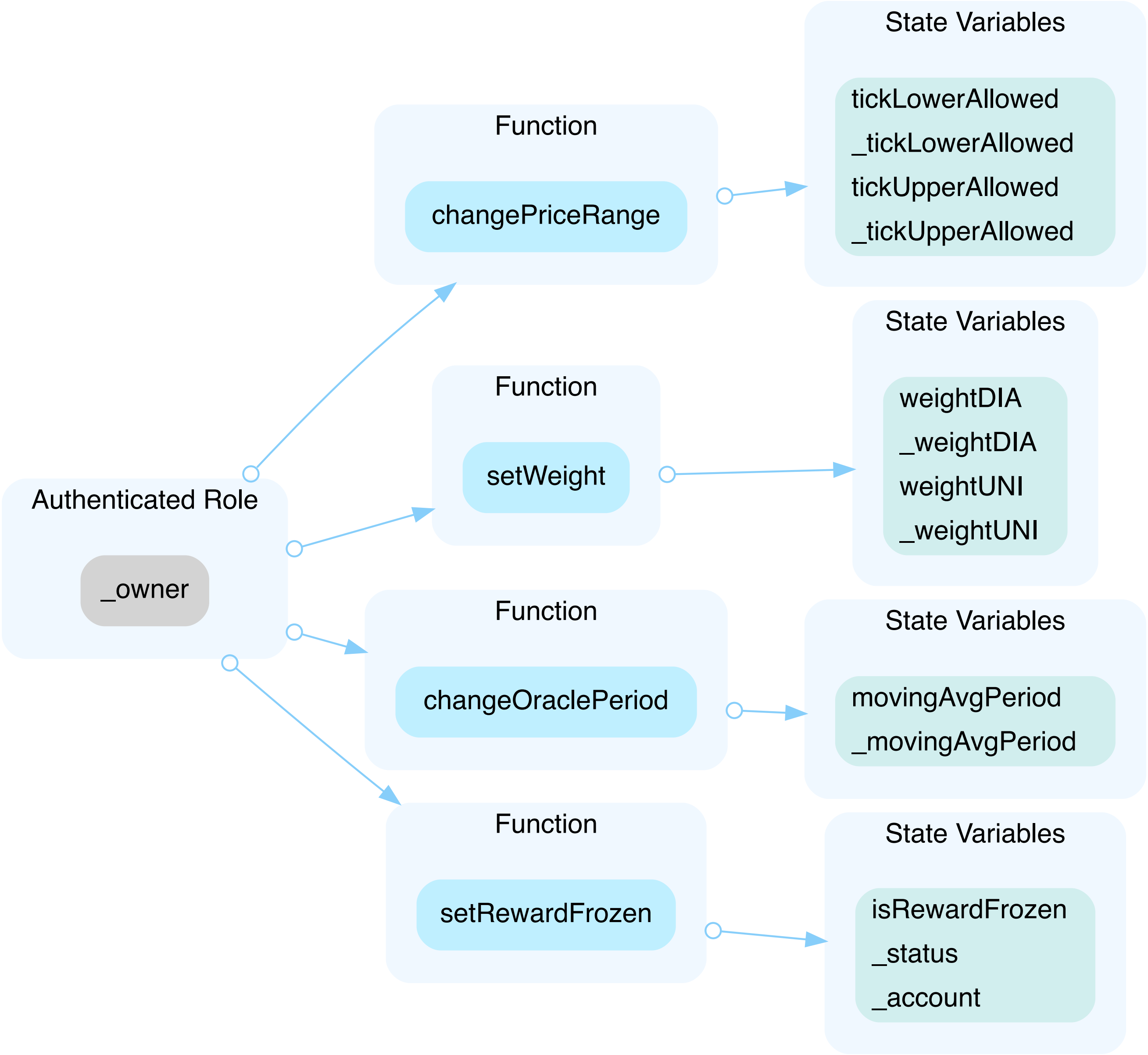
In the contract, `LPStaking`, the role, `_owner`, has the authority over the functions shown in the diagram below.

Any compromise to the privileged account which has access to `_owner` may allow the hacker to take advantage of this.



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

Any compromise to the privileged account which has access to `_owner` may allow the hacker to take advantage of this.



Recommendation

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 to be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., Multisignature wallets.

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

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

- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

[Sperax Team]:

1. Any function in which the _owner role can adjust can't move any of user funds. These functions are in place so the Sperax can adjust certain deposit parameters to make the experience more enjoyable and profitable for the end user. Under no circumstance can the Sperax team withdraw user funds.
2. _owner account is a Gnosis Safe multi-sig account that is controlled by three different, independent accounts. No privileged function can be triggered unless all of three accounts sign and approve the transaction. There is no single point of failure.
3. Shortly after USDs and Liquidity Mining launch, the _owner role will be transferred from the Gnosis Safe multi-sig to Sperax DAO. The access to the functions mentioned above will then become fully decentralized with the protection of a 48-hour timelock mechanism.

SPA-02 | Redundant Code Components

Category	Severity	Location	Status
Volatile Code	● Informational	contract/farm_SPA_USDs.sol (fe7bde7): 110~112	ⓘ Acknowledged

Description

The linked statements do not affect the functionality of the codebase and appear to be either leftover from test code or older functionality.

Recommendation

We advise to remove the redundant statements for production environments.

Alleviation

Sperax team acknowledged this finding.

SPA-03 | Variables that could be declared as `constant`

Category	Severity	Location	Status
Gas Optimization	● Informational	contract/farm_SPA_USDs.sol (fe7bde7): 48, 49	ⓘ Acknowledged

Description

The linked variables could be declared as `constant` since these state variables are never modified.

Recommendation

We recommend to declare these variables as `constant`.

Alleviation

Sperax team acknowledged this finding.

SPA-04 | Unknown Imported Source File

Category	Severity	Location	Status
Logical Issue	● Minor	contract/farm_SPA_USDs.sol (fe7bde7): 12~13	ⓘ Acknowledged

Description

The imported source files below

```
12  import "../libraries/library.sol";
13  import "../interfaces/IDIAOracle.sol";
```

are not exist, and the file `library.sol` is not truly used.

Recommendation

Consider importing the missing source files.

Alleviation

Sperax team acknowledged this finding.

SPA-05 | Third Party Dependencies

Category	Severity	Location	Status
Volatile Code	● Minor	contract/farm_SPA_USDs.sol (fe7bde7): 31~34	ⓘ Acknowledged

Description

The contract is serving as the underlying entity to interact with third-party `UniswapV3`, 'Openzeppelin' and `DIAOracle` protocols. 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 this contract requires interaction with `UniswapV3`, 'Openzeppelin', `DIAOracle`, etc. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Alleviation

Sperax team acknowledged this finding.

SPA-06 | Extensive precision conversion

Category	Severity	Location	Status
Mathematical Operations	● Informational	contract/farm_SPA_USDs.sol (fe7bde7): 40~42	ⓘ Acknowledged

Description

The contract contains a large number of precision conversion calculations, such as the following code:

```
40 uint public constant USDs_PER_SPA_PREC = 10**18;
41 uint public constant USDC_PER_SPA_PREC = 10**18;
42 uint public constant USDs_PER_USDC_PREC = 10**18;
```

We have doubts about the accuracy of these three price pairs. We hope that the project team will pay more attention and do more tests.

Alleviation

Sperax 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.

Mathematical Operations

Mathematical Operation findings relate to mishandling of math formulas, such as overflows, incorrect operations etc.

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.

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.