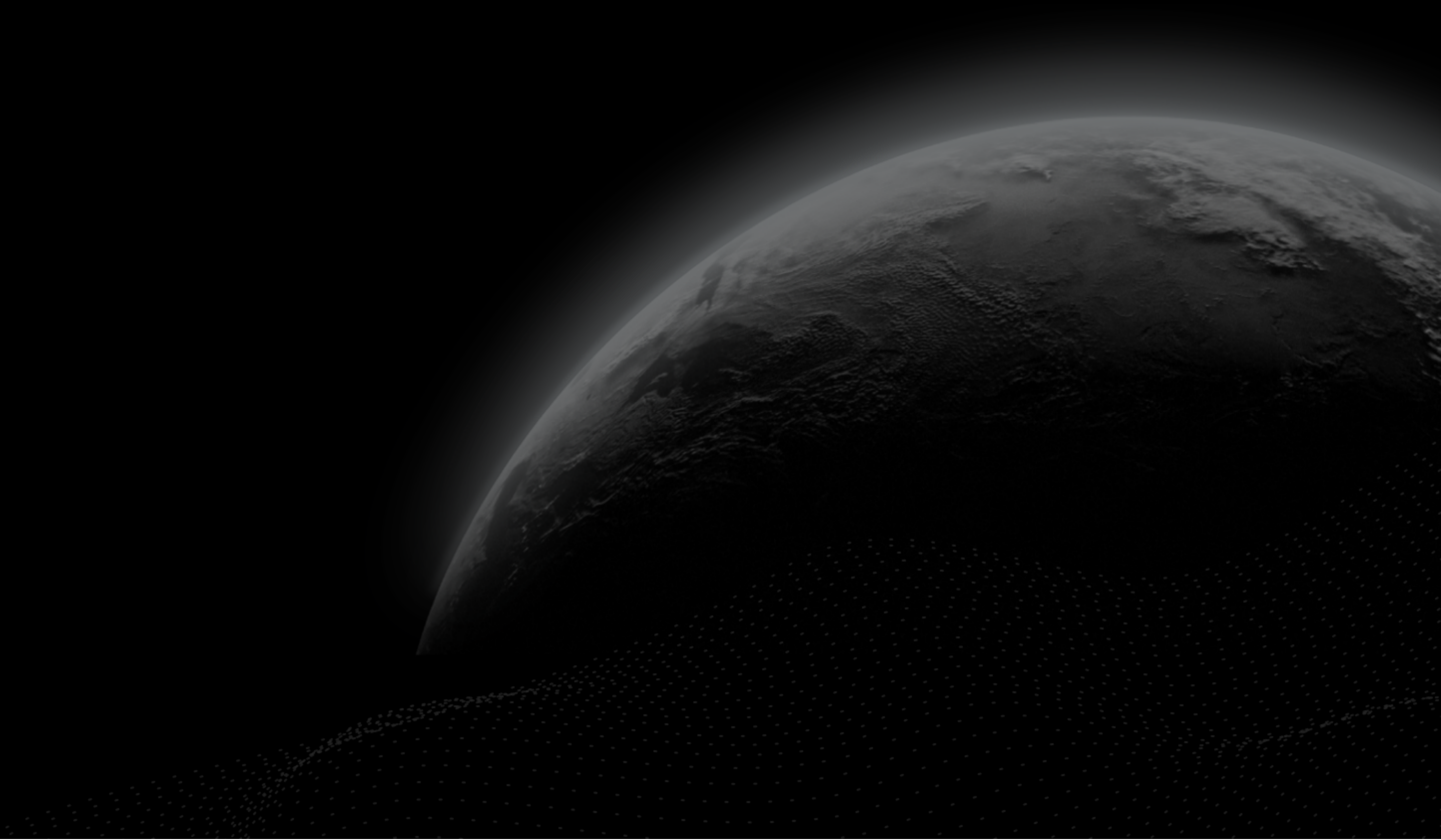
Security Assessment

Venus - sfrxETH oracle adapter

CertiK Assessed on May 17th, 2024



CertiK Assessed on May 17th, 2024

Venus - sfrxETH oracle adapter

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Binance Smart Chain (BSC)	Manual Review, Static Analysis
LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 05/17/2024	N/A

CODEBASE

https://github.com/VenusProtocol/oracle/

View All in Codebase Page

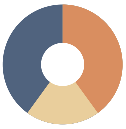
COMMITS

Base: 54462b89a393d478f90d1154134d6c75d27753f5

update: b24ef729a7f1b13d1c2b572e4717612275659dd1

View All in Codebase Page

Vulnerability Summary



Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined
5	2	0	0	3	0

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
2	Major	2 Acknowledged	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
0	Medium		Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
1	Minor	1 Resolved	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
2	Informational	1 Resolved, 1 Acknowledged	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | VENUS - SFRXETH ORACLE ADAPTER

CODEBASE | VENUS - SFRXETH ORACLE ADAPTER

Repository

https://github.com/VenusProtocol/oracle/

Commit

Base: 54462b89a393d478f90d1154134d6c75d27753f5

update: b24ef729a7f1b13d1c2b572e4717612275659dd1

AUDIT SCOPE | VENUS - SFRXETH ORACLE ADAPTER

1 file audited ● 1 file with Acknowledged findings

ID	Repo	File	SHA256 Checksum
● SFE	VenusProtocol/oracle	contracts/oracles/SFrxETHOracle.sol	5552038aa01ee92250074434eefbdea379ad24657c2d81e073e335abce94f34e

APPROACH & METHODS | VENUS - SFRXETH ORACLE ADAPTER

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

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

SUMMARY | VENUS - SFRXETH ORACLE ADAPTER

This audit concerns the changes made in PR-191.

In particular, this PR was refactor the `SFrxETHOracle` contract to utilize the `SfrxEthUsdDualOracle` deployed at 0x3d3d868522b5a4035adcb67bf0846d61597a6a6f.

When `getPrice()` is called, if the input asset is `SFRXETH`, it calls `getPrices()` from the `SfrxEthUsdDualOracle`, which is designed to return prices from two different oracles and has the following return values:

```
(bool _isBadData, uint256 _priceLow, uint256 _priceHigh)
```

Where the `_isBadData` is true when data is stale or otherwise bad, `_priceLow` is the lower of the two prices, and `_priceHigh` is the higher of the two price. It then reverts if `_isBadData` is true. The prices are the amount of `SFrxEth` per 1 dollar, so it then inverts them to give the high and low price of `SFrxEth` in USD and checks that the two prices are within a configurable maximum difference. This helps limit the amount that one of the oracles can be manipulated before causing a revert. Finally it returns the average of the two prices.

DEPENDENCIES | VENUS - SFRXETH ORACLE ADAPTER

Third Party Dependencies

The protocol is serving as the underlying entity to interact with third party protocols. The third parties that the contracts interact with are:

- `SfrxEthUsdDualOracle`

The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. Moreover, updates to the state of a project contract that are dependent on the read of the state of external third party contracts may make the project vulnerable to read-only reentrancy. In addition, upgrades of third parties can possibly create severe impacts, such as increasing fees of third parties, migrating to new LP pools, etc.

Assumptions

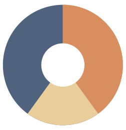
Within the scope of the audit, assumptions are made about the intended behavior of the protocol in order to inspect consequences based on those behaviors. Assumptions made within the scope of this audit include:

- `SFRXETH_FRAX_ORACLE` is set to the contract at address 0x3d3d868522b5a4035adcb67bf0846d61597a6a6f
- `SFRXETH` is set to the contract at address 0xac3E018457B222d93114458476f3E3416Abbe38F

Recommendations

We recommend constantly monitoring the third parties involved to mitigate any side effects that may occur when unexpected changes are introduced, as well as vetting any third party contracts used to ensure no external calls can be made before updates to its state. Additionally, we recommend all assumptions about the behavior of the project are thoroughly reviewed and, if the assumptions do not match the intention of the protocol, documenting the intended behavior for review.

FINDINGS | VENUS - SFRXETH ORACLE ADAPTER



5	0	2	0	1	2
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - sfrxETH oracle adapter. Through this audit, we have uncovered 5 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
SFE-01	**Centralized Control Of Contract Upgrade**	**Centralization**	**Major**	● **Acknowledged**
SFE-02	**Centralization Related Risks**	**Centralization**	**Major**	● **Acknowledged**
SFE-03	Unprotected Initializer	Coding Issue	Minor	● Resolved
SFE-04	Dependency On Choice For `maxAllowedPriceDifference`	Design Issue	Informational	● Acknowledged
SFE-05	Missing Zero Value Check	Logical Issue	Informational	● Resolved

SFE-01 | CENTRALIZED CONTROL OF CONTRACT UPGRADE

Category	Severity	Location	Status
Centralization	● **Major**	**contracts/oracles/SFrxETHOracle.sol: 47~53**	● **Acknowledged**

Description

`SFrxETHOracle` is an upgradeable contract, the owner can upgrade the contracts at any time. If an attacker compromises the owner, they can change the implementation of the contract to return any price they wish for the asset to steal funds from the protocol.

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

`[Venus, 05/16/2024]` : "The owner of SFrxETHOracle will be initially the Guardian wallet [1] on Ethereum. This ownership will be transferred to a Normal Timelock contract on Ethereum, as soon as the Multichain Governance system [2] is deployed to Ethereum. From that moment, the upgrade will be doable only via Governance."

[1] https://etherscan.io/address/0x285960C5B22fD66A736C7136967A3eB15e93CC67

[2] https://docs-v4.venus.io/technical-reference/reference-technical-articles/multichain-governance

`[CertiK, 05/17/2024]` : Once the ownership is transferred to the Normal Timelock it will meat our mitigation standards. However, until that time we will mark this finding as *Acknowledged*.

SFE-02 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	● **Major**	**contracts/oracles/SFrxETHOracle.sol: 60**	● **Acknowledged**

Description

In the contract `SFrxETHOracle` , the role `DEFAULT_ADMIN_ROLE` of the `AccessControlManager` can grant addresses the privilege to call the following functions:

- `setMaxAllowedPriceDifference()`

Any compromise to the `DEFAULT_ADMIN_ROLE` or accounts granted this privilege may allow a hacker to take advantage of this authority and do the following:

- Increase or decrease the allowed price difference to cause a denial of service or enable larger price fluctuations.

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

`[Venus, 05/16/2024]` : "The AccessControlManager contract used on Ethereum is [1], where the DEFAULT_ADMIN_ROLE is assigned to the Guardian wallet [2]. After deploying the Multichain Governance system [3] to Ethereum, the DEFAULT_ADMIN_ROLE will be transferred to a Normal Timelock contract, so only Governance will be able to grant addresses the privilege to call the mentioned function."

[1] https://etherscan.io/address/0x230058da2D23eb8836EC5DB7037ef7250c56E25E

[2] https://etherscan.io/address/0x285960C5B22fD66A736C7136967A3eB15e93CC67

[3] https://docs-v4.venus.io/technical-reference/reference-technical-articles/multichain-governance

`[CertiK, 05/17/2024]` : Once the DEFAULT_ADMIN_ROLE is transferred to the Normal Timelock and if the function privledges have only been given to secure accounts, it will meat our mitigation standards. However, until that time we will mark this finding as *Acknowledged*.

SFE-03 | UNPROTECTED INITIALIZER

Category	Severity	Location	Status
Coding Issue	● Minor	contracts/oracles/SFrxETHOracle.sol: 38~53	● Resolved

Description

The contract `SFrxETHOracle` does not protect its `initializer` . An attacker can call the initializer and assume ownership of the logic contract, whereby they can perform privileged operations that trick unsuspecting users into believing that they are the owner of the upgradeable contract.

Recommendation

We recommend calling `_disableInitializers()` in the constructor to be consistent with other contracts in the repository.

Alleviation

`[CertiK, 05/16/2024]` : The client made changes resolving the finding in commit b24ef729a7f1b13d1c2b572e4717612275659dd1.

SFE-04 DEPENDENCY ON CHOICE FOR `maxAllowedPriceDifference`

Category	Severity	Location	Status
Design Issue	● Informational	contracts/oracles/SFrxETHOracle.sol: 62~63	● Acknowledged

Description

The `maxAllowedPriceDifference` is designed to revert cases when the difference of the two prices returned via the `SfrxEthUsdDualOracle` are greater than it. This helps mitigate issues if one oracle was to be compromised and return the wrong price. However, this value must be chosen high enough that it will not cause a denial of service due to natural discrepancies between the two oracles prices and low enough that it will not allow for a significant manipulated price to be returned.

Recommendation

We recommend constantly monitoring the underlying oracles behind `SfrxEthUsdDualOracle` and adjusting the `maxAllowedPriceDifference` as appropriate.

Alleviation

`[Venus, 05/16/2024]` : "Issue acknowledged. I won't make any changes for the current version."

SFE-05 | MISSING ZERO VALUE CHECK

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/oracles/SFrxETHOracle.sol: 78~79, 79~80	● Resolved

Description

While it is unlikely, it is theoretically possible for the returned `priceLow` and `priceHigh` values to be large enough that they exceed the value `EXP_SCALE ** 2` , causing `priceHighInUSD` and `priceLowInUSD` respectively to be 0.

While the resilient oracle contract ensures the returned price is nonzero, it is convention within other contracts to make this check sooner within the logic.

Recommendation

We recommend ensuring that each of `priceHighInUSD` and `priceLowInUSD` are nonzero, so that the logic can revert sooner if this is the case.

Alleviation

`[CertiK, 05/16/2024]` : The client made changes resolving the finding in commit 6130942986f3e75725ea295b1e634c73df1601da.

APPENDIX | VENUS - SFRXETH ORACLE ADAPTER

Finding Categories

Categories	Description
Coding Issue	Coding Issue findings are about general code quality including, but not limited to, coding mistakes, compile errors, and performance issues.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

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 | CERTIK

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.

CertiK | **Securing** the **Web3** World

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.