



Venus - Core Contracts Upgrade

Security Assessment

CertiK Assessed on Aug 24th, 2025





Certik Assessed on Aug 24th, 2025

Venus - Core Contracts Upgrade

The security assessment was prepared by Certik.

Executive Summary

TYPES

Lending

ECOSYSTEM

Binance Smart Chain
(BSC)

METHODS

Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Preliminary comments published on 08/24/2025

Final report published on 08/24/2025

Vulnerability Summary



9

Total Findings

9

Resolved

0

Partially Resolved

0

Acknowledged

0

Declined

0 Centralization

Centralization findings highlight privileged roles & functions and their capabilities, or instances where the project takes custody of users' assets.

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.

0 Major

Major risks may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.

0 Medium

Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.

2 Minor

2 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.

7 Informational

7 Resolved



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 - CORE CONTRACTS UPGRADE

Summary

[Executive Summary](#)

[Vulnerability Summary](#)

[Codebase](#)

[Audit Scope](#)

[Approach & Methods](#)

Overview

Findings

[VCC-05 : Interfaces Have Inconsistent Return Types](#)

[VCC-06 : Proxy Contracts Fallback Is No Longer Payable](#)

[VCC-02 : IWBNNB Is Not Longer Needed In `VBNBStorage.sol` File](#)

[VCC-03 : Inconsistent Use Of Specific Imports](#)

[VCC-07 : Files Missing SPDX License Identifier](#)

[VCC-08 : Both IPrime.Sol And IPrimeV5.Sol Have Same Contract Name](#)

[VCC-09 : Typos And Inconsistencies](#)

[VCC-10 : Inconsistent Use Of Pure And View](#)

[VCC-11 : Implicit Changing Of ABIEncoder](#)

Optimizations

[VCC-01 : Unnecessary Imports](#)

Appendix

Disclaimer

CODEBASE | VENUS - CORE CONTRACTS UPGRADE

Repository

<https://github.com/VenusProtocol/venus-protocol>

Commit

Base: [1bd44b21f49c611b554349364e33ac43d51e4506](#)

Update1: [41eaa040d54e19cff1fc73906ea3bddc4e29150e](#)

Update2: [36bfad1f29fed11f775b3d927189f832b788cef8](#)

Audit Scope

The file in scope is listed in the appendix.

APPROACH & METHODS | VENUS - CORE CONTRACTS UPGRADE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Core Contracts Upgrade 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.

OVERVIEW | VENUS - CORE CONTRACTS UPGRADE

This audit concerns the changes made in files outlined in the following PRs:

- [PR-607](#)

Note that any centralization risks present in the existing codebase before these PRs were not considered in this audit and only those added in these PRs are addressed in the audit. We recommend all users carefully review the centralization risks, much of which can be found in our previous audits, which can be found here: <https://skynet.certik.com/projects/venus>.

PR-607

This PR is designed to upgrade the solidity version in the Comptroller, Lens, VAIController, and VTokens to 0.8.25 while not making any breaking changes to the contracts interfaces.

FINDINGS | VENUS - CORE CONTRACTS UPGRADE



9
Total Findings

0
Critical

0
Centralization

0
Major

0
Medium

2
Minor

7
Informational

This report has been prepared for Venus to identify potential vulnerabilities and security issues within the reviewed codebase. During the course of the audit, a total of 9 issues were identified. Leveraging a combination of Manual Review & Static Analysis the following findings were uncovered:

ID	Title	Category	Severity	Status
VCC-05	Interfaces Have Inconsistent Return Types	Inconsistency	Minor	Resolved
VCC-06	Proxy Contracts Fallback Is No Longer Payable	Inconsistency	Minor	Resolved
VCC-02	IWBNB Is Not Longer Needed In <code>VBNBStorage.sol</code> File	Inconsistency	Informational	Resolved
VCC-03	Inconsistent Use Of Specific Imports	Inconsistency	Informational	Resolved
VCC-07	Files Missing SPDX License Identifier	Coding Style	Informational	Resolved
VCC-08	Both IPrime.Sol And IPrimeV5.Sol Have Same Contract Name	Coding Style	Informational	Resolved
VCC-09	Typos And Inconsistencies	Inconsistency	Informational	Resolved
VCC-10	Inconsistent Use Of Pure And View	Logical Issue	Informational	Resolved
VCC-11	Implicit Changing Of ABIEncoder	Inconsistency	Informational	Resolved

VCC-05 | Interfaces Have Inconsistent Return Types

Category	Severity	Location	Status
Inconsistency	Minor	contracts/Tokens/VAI/IVAI.sol (Base): 8; contracts/Tokens/VAI/VAI.sol (Base): 24; contracts/Tokens/XVS/IXVS.sol (Base): 28~29, 31~35; contracts/Tokens/XVS/XVS.sol (Base): 37, 39~45	Resolved

Description

IVAI

In the interface IVAI, the function `wards()` returns type `bool`. However, in the contract `VAI`, `wards` is a mapping from an `address` to a `uint256` so that the return value is a `uint256`. While only the values of 0 and 1 are assigned, we recommend keeping the interface consistent with the implementation. If the code is adapted to return other `uint256` values in the future, then contracts that use the interface may revert unexpectedly.

IXVS

In the interface IXVS, the function `numCheckpoints()` returns type `uint256`. However, in the contract `XVS`, `numCheckpoints` is a mapping from an `address` to a `uint32`. While the `uint32` will be implicitly cast as a `uint256`, we recommend keeping the interfaces return values consistent to ensure proper integration.

In the interface IXVS, the functions `DOMAIN_TYPEHASH()` and `DELEGATION_TYPEHASH()` returns type `string`. However, in the contract `XVS` they return a type `bytes32` which is not implicitly convertible to a `string`. As such if the interface is used to interact with `XVS` contract to call `DOMAIN_TYPEHASH()` or `DELEGATION_TYPEHASH()` it will revert.

Recommendation

We recommend ensuring that all interface return types match the return types used in their implementing contracts. Furthermore, we recommend having contracts inherit their interfaces when possible to ensure consistency.

Alleviation

[CertiK, 08/21/2025]: The client made the recommended changes resolving this finding in commit [247596d13184f8f6e248fa678d9bac0fb0e2c6d2](#).

VCC-06 | Proxy Contracts Fallback Is No Longer Payable

Category	Severity	Location	Status
Inconsistency	Minor	contracts/Comptroller/Diamond/Diamond.sol (Base): 251; contracts/Comptroller/Unitroller.sol (Base): 133; contracts/Tokens/VAI/VAIUnitroller.sol (Base): 133; contracts/Tokens/VTokens/VBep20Delegator.sol (Base): 67	Resolved

Description

All `fallback()` functions in the proxy contracts have been updated for the new Solidity version, but the `payable` modifier has been removed. As a result, any external call to the proxy contracts with a nonzero `msg.value` will revert, blocking the transfer of BNB through these proxies. This change will prevent any functionality involving native BNB to be supported via the proxy.

Recommendation

We recommend ensuring that this is the desired behavior or adding the payable keyword.

Alleviation

[Venus, 08/20/2025]: This is the desired behaviour. We won't send native BNB to these contracts.

VCC-02 | IWBNNB Is Not Longer Needed In VBNBStorage.sol File

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/Admin/VBNBAdminStorage.sol (Base): 4, 17~19	● Resolved

Description

The IWBNNB interface is now included in the external folder and contracts no longer fetch it from the VBNBAdminStorage.sol file. As such it can be removed from the file.

Recommendation

We recommend removing the unused interface from the file and instead referencing the one in the external folder when needed.

Alleviation

[CertiK, 08/21/2025]: The client made the recommended changes resolving this finding in commit [6e096557283961f3b42228a50ee874cf656dc5bb](#).

VCC-03 | Inconsistent Use Of Specific Imports

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/Admin/VBNBAdmin.sol (Base): 4~6; contracts/Comptroller/ComptrollerLensInterface.sol (Base): 3; contracts/Comptroller/Diamond/DiamondConsolidated.sol (Base): 3~7; contracts/Comptroller/Unitroller.sol (Base): 3~4; contracts/Lens/ComptrollerLens.sol (Base): 5, 8~11; contracts/Liquidator/Liquidator.sol (Base): 9, 12; contracts/Tokens/VAI/VAIUnitroller.sol (Base): 3~4; contracts/Utils/Exponential.sol (Base): 3~4; contracts/XVSVault/XVSVault.sol (Base): 6~13; contracts/XVSVault/XVSVaultStorage.sol (Base): 3~5	● Resolved

Description

Throughout the codebase specific imports are used, however, the cited lines do not use specific imports.

Recommendation

We recommend using specific imports for all imports for consistency.

Alleviation

[CertiK, 08/24/2025]: The client made the recommended changes in commits

- [a37766fac4dcdf0b9e30f1e088a70ce307e6bf60](#);
- [3cdea60a9e0206a7b2ccf0454743e72a6792affb](#);
- [36bfad1f29fed11f775b3d927189f832b788cef8](#).

VCC-07 | Files Missing SPDX License Identifier

Category	Severity	Location	Status
Coding Style	● Informational	contracts/Comptroller/ComptrollerInterface.sol (Base): 1; contracts/Comptroller/ComptrollerLensInterface.sol (Base): 1; contracts/Comptroller/Diamond/DiamondConsolidated.sol (Base): 1; contracts/Comptroller/Unitroller.sol (Base): 1; contracts/Lens/ComptrollerLens.sol (Base): 1; contracts/Lens/SnapshotLens.sol (Base): 1; contracts/Lens/VenusLens.sol (Base): 1; contracts/Oracle/PriceOracle.sol (Base): 1; contracts/Tokens/VAI/VAIControllerInterface.sol (Base): 1; contracts/Tokens/VAI/VAIControllerStorage.sol (Base): 1; contracts/Tokens/VAI/VAIUnitroller.sol (Base): 1; contracts/Tokens/VTokens/VBNB.sol (Base): 1; contracts/Tokens/VTokens/VBep20.sol (Base): 1; contracts/Tokens/VTokens/VBep20Delegate.sol (Base): 1; contracts/Tokens/VTokens/VBep20Delegator.sol (Base): 2; contracts/Tokens/VTokens/VBep20Immutable.sol (Base): 1; contracts/Tokens/VTokens/VToken.sol (Base): 1; contracts/Tokens/VTokens/VTokenInterfaces.sol (Base): 1~2; contracts/Tokens/XVS/IXVS.sol (Base): 1; contracts/Utils/CarefulMath.sol (Base): 1; contracts/Utils/ErrorReporter.sol (Base): 1; contracts/Utils/Exponential.sol (Base): 1; contracts/Utils/ExponentialNoError.sol (Base): 1; contracts/XVSVault/XVSVaultStorage.sol (Base): 1~2	● Resolved

Description

Some file lack an SPDX License Identifier, which is required for clarity on the licensing conditions under which the code is released. This omission may cause ambiguity about rights to use, modify, and distribute the source code. For broader compatibility and transparency, the SPDX License Identifier should be specified at the top of each Solidity file.

Recommendation

We recommend adding a SPDX License Identifier for all files.

Alleviation

[CertiK, 08/21/2025]: The client made the recommended changes resolving the finding in commits

- [24b58bc883c48ac990c218d6d6522c1b2b0262f3](#)
- [67b942091ca9ab8af2ecce4a536b8c5f810a193d](#)

VCC-08 | Both IPrime.Sol And IPrimeV5.Sol Have Same Contract Name

Category	Severity	Location	Status
Coding Style	● Informational	contracts/Tokens/Prime/IPrimeV5.sol (Base): 10	● Resolved

Description

Both `IPrime.sol` and `IPrimeV5.sol` define an interface with the identical name `IPrime`, differing only in compiler version. This duplication can create confusion for developers and tooling, potentially leading to accidental usage of the wrong interface version, especially in larger or evolving codebases. Distinguishing interface names helps ensure clear versioning and reduces the risk of integration errors.

Recommendation

We recommend that the interfaces in `IPrime.sol` and `IPrimeV5.sol` are given distinct, version-specific names to clearly differentiate between the two.

Alleviation

[CertiK, 08/21/2025]: The client made the recommended changes resolving this finding in commit [ba8b206e2df2ff2ad7cd76a8646dbe01898781de](#).

VCC-09 | Typos And Inconsistencies

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/Tokens/VAI/VAIController.sol (Base): 315; contracts/Tokens/VTokens/VBep20Delegator.sol (Base): 215, 341; contracts/Tokens/VTokens/VToken.sol (Base): 93, 264, 1188, 1310	● Resolved

Description

Comments refer to using `-1` to represent the maximum value, but with the updated compiler, `-1` is no longer valid for this purpose. The contract now correctly uses `type(uint256).max` to denote the maximum value, but outdated comments referencing `-1` could mislead developers reviewing or maintaining the code. This inconsistency between comments and implementation may result in misunderstandings or incorrect usage patterns when interacting with these sections of the contract.

Recommendation

We recommend updating the comments to reference the `type(uint256).max` or `2^256-1` as opposed to `-1` to avoid any confusion.

Alleviation

[CertiK, 08/21/2025]: The client made the recommended changes resolving this finding in commit [735fdd238914f493a261f8a091387ed48333243f](https://github.com/venusprotocol/venus-core/commit/735fdd238914f493a261f8a091387ed48333243f).

VCC-10 | Inconsistent Use Of Pure And View

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/Tokens/VAI/IVAI.sol (Base): 29; contracts/Tokens/VAI/VAI.sol (Base): 40~43	● Resolved

Description

The sited lines above mark functions as view when they reference constants and can be marked pure.

Recommendation

We recommend marking these function pure to be consistent.

Alleviation

[CertiK, 08/21/2025]: The client made the recommended changes resolving this finding in commit [9c1ea7257e05725869132e06d82ee32a8ae466d8](#).

VCC-11 | Implicit Changing Of ABIEncoder

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/Comptroller/ComptrollerInterface.sol (Base): 1; contracts/Comptroller/ComptrollerStorage.sol (Base): 3; contracts/Comptroller/Diamond/facets/FacetBase.sol (Base): 3; contracts/Comptroller/Diamond/facets/MarketFacet.sol (Base): 3; contracts/Comptroller/Diamond/facets/PolicyFacet.sol (Base): 3; contracts/Comptroller/Diamond/facets/RewardFacet.sol (Base): 3; contracts/Comptroller/Diamond/facets/SetterFacet.sol (Base): 3; contracts/Comptroller/Diamond/facets/XVSRewardsHelper.sol (Base): 3; contracts/Comptroller/Diamond/interfaces/IMarketFacet.sol (Base): 3; contracts/Comptroller/Diamond/interfaces/IPolicyFacet.sol (Base): 3; contracts/Comptroller/Diamond/interfaces/IRewardFacet.sol (Base): 3; contracts/Comptroller/Diamond/interfaces/ISetterFacet.sol (Base): 3; contracts/Comptroller/Unitroller.sol (Base): 1; contracts/Tokens/VAI/VAIController.sol (Base): 2; contracts/Tokens/VAI/VAIControllerInterface.sol (Base): 1; contracts/Tokens/VAI/VAIControllerStorage.sol (Base): 1; contracts/Tokens/VAI/VAIUnitroller.sol (Base): 1; contracts/Tokens/VTokens/VBNB.sol (Base): 1; contracts/Tokens/VTokens/VBep20.sol (Base): 1; contracts/Tokens/VTokens/VBep20Delegate.sol (Base): 1, 1; contracts/Tokens/VTokens/VBep20Delegator.sol (Base): 1; contracts/Tokens/VTokens/VBep20Immutable.sol (Base): 1; contracts/Tokens/VTokens/VToken.sol (Base): 1; contracts/Tokens/VTokens/VTokenInterfaces.sol (Base): 1; contracts/Utils/CarefulMath.sol (Base): 1; contracts/Utils/ErrorHandler.sol (Base): 1; contracts/Utils/ExponentialNoError.sol (Base): 1	● Resolved

Description

Since solidity version 0.8.0 the `ABIEncoderV2` is used by default. As such, due to the solidity version change, some of the contracts implicitly change from using `ABIEncoderV1` to `ABIEncoderV2`.

Recommendation

We recommend ensuring that the implicit changing of the ABIEncoder is intended.



Alleviation

[Venus, 08/20/2025]: This is the intended behaviour.

OPTIMIZATIONS | VENUS - CORE CONTRACTS UPGRADE

ID	Title	Category	Severity	Status
VCC-01	Unnecessary Imports	Code Optimization	Optimization	● Resolved

VCC-01 | Unnecessary Imports

Category	Severity	Location	Status
Code Optimization	 Optimization	contracts/Comptroller/Diamond/interfaces/IFacetBase.sol (Base): 5~12, 13; contracts/Lens/ComptrollerLens.sol (Base): 3~5	 Resolved

Description

In the `IFacetBase` interface it imports from many files, however, it only needs to import `Action` as all other items are imported in the implementation of `FacetBase`.

In the `ComptrollerLens` it imports `ResilientOracleInterface` and `VBep20.sol`, however, it does not use these and they can be removed.

Recommendation

We recommend removing the unnecessary imports.

Alleviation




















[CertiK, 08/24/2025]: The client made the recommended changes in commits

- [69d086846d02ba96b2e668ab84313672d3c03a04](#);
- [36bfad1f29fed11f775b3d927189f832b788cef8](#).























APPENDIX | VENUS - CORE CONTRACTS UPGRADE

Audit Scope









VenusProtocol/venus-protocol

-  contracts/Admin/VBNBAdmin.sol
-  contracts/Admin/VBNBAdminStorage.sol
-  contracts/Comptroller/Diamond/facets/FacetBase.sol
-  contracts/Comptroller/Diamond/facets/MarketFacet.sol
-  contracts/Comptroller/Diamond/facets/PolicyFacet.sol
-  contracts/Comptroller/Diamond/facets/RewardFacet.sol
-  contracts/Comptroller/Diamond/facets/SetterFacet.sol
-  contracts/Comptroller/Diamond/facets/XVSRewardsHelper.sol
-  contracts/Comptroller/Diamond/interfaces/IFacetBase.sol
-  contracts/Comptroller/Diamond/interfaces/IMarketFacet.sol
-  contracts/Comptroller/Diamond/interfaces/IPolicyFacet.sol
-  contracts/Comptroller/Diamond/interfaces/IRewardFacet.sol
-  contracts/Comptroller/Diamond/interfaces/ISetterFacet.sol
-  contracts/Comptroller/Diamond/Diamond.sol
-  contracts/Comptroller/Diamond/DiamondConsolidated.sol
-  contracts/Comptroller/ComptrollerInterface.sol
-  contracts/Comptroller/ComptrollerLensInterface.sol
-  contracts/Comptroller/ComptrollerStorage.sol
-  contracts/Comptroller/Unitroller.sol

VenusProtocol/venus-protocol

-  contracts/Lens/ComptrollerLens.sol
-  contracts/Lens/SnapshotLens.sol
-  contracts/Lens/VenusLens.sol
-  contracts/Liquidator/Liquidator.sol
-  contracts/Oracle/PriceOracle.sol
-  contracts/Tokens/Prime/IPrimeV5.sol
-  contracts/Tokens/VAI/IVAI.sol
-  contracts/Tokens/VAI/VAIController.sol
-  contracts/Tokens/VAI/VAIControllerInterface.sol
-  contracts/Tokens/VAI/VAIControllerStorage.sol
-  contracts/Tokens/VAI/VAIUnitroller.sol
-  contracts/Tokens/VTokens/VBep20.sol
-  contracts/Tokens/VTokens/VBep20Delegate.sol
-  contracts/Tokens/VTokens/VBep20Delegator.sol
-  contracts/Tokens/VTokens/VBep20Immutable.sol
-  contracts/Tokens/VTokens/VBNB.sol
-  contracts/Tokens/VTokens/VToken.sol
-  contracts/Tokens/VTokens/VTokenInterfaces.sol
-  contracts/Tokens/XVS/IXVS.sol
-  contracts/Utils/CarefulMath.sol
-  contracts/Utils/ErrorReporter.sol
-  contracts/Utils/Exponential.sol

VenusProtocol/venus-protocol

	contracts/Utils/ExponentialNoError.sol
	contracts/XVSVault/XVSVault.sol
	contracts/XVSVault/XVSVaultStorage.sol
	contracts/Comptroller/Diamond/interfaces/IDiamondCut.sol
	contracts/external/IProtocolShareReserve.sol
	contracts/external/IWBNB.sol
	contracts/Tokens/Prime/IPrime.sol
	contracts/InterfacesV8.sol

Finding Categories

Categories	Description
Coding Style	Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable.
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.

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.

Elevating Your **Web3** Journey

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is the largest 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.

