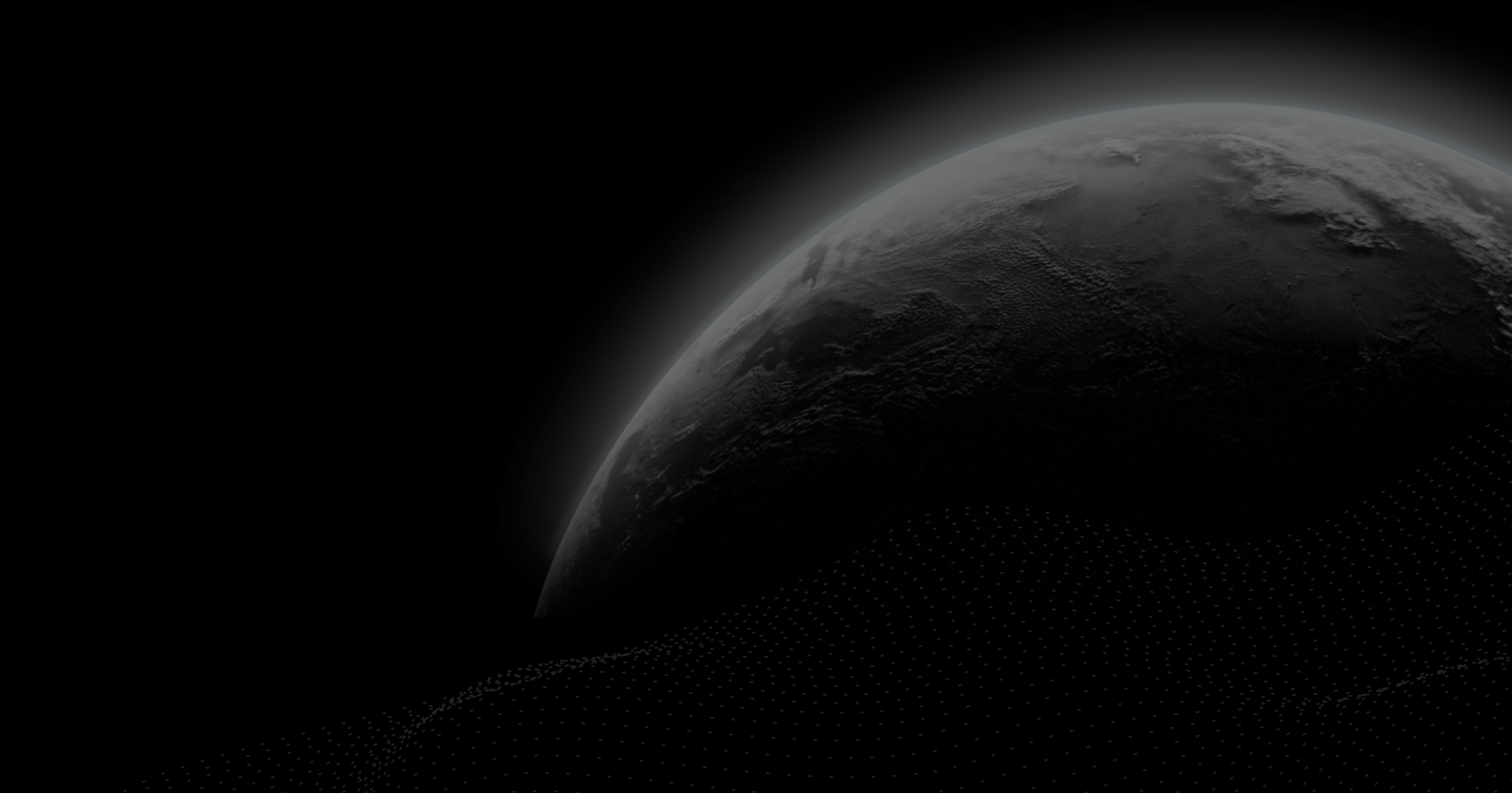
CERTIK

Security Assessment

Venus - Mesh Architecture

CertiK Assessed on Apr 19th, 2024



CertiK Assessed on Apr 19th, 2024

Venus - Mesh Architecture

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Ethereum (ETH) | opBNB	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Solidity	Delivered on 04/19/2024	N/A

CODEBASE
https://github.com/VenusProtocol/vips
View All in Codebase Page

COMMITS
base-opbnb: 2468c5ba5c1606f42a0536531a291dab53b91cc3
base-ethereum: a6a75f847746993c10a49ed97865c3a9162c71b4
Update: a46cf94d7072726edee388d9cd6327a933dcaa17
View All in Codebase Page

Vulnerability Summary

3	2	0	0	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

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 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.
0	Minor		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.
3	Informational	2 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 - MESH ARCHITECTURE

CODEBASE | VENUS - MESH ARCHITECTURE

Repository

https://github.com/VenusProtocol/vips

Commit

base-opbnb: 2468c5ba5c1606f42a0536531a291dab53b91cc3

base-ethereum: a6a75f847746993c10a49ed97865c3a9162c71b4

Update: a46cf94d7072726edee388d9cd6327a933dcaa17

AUDIT SCOPE | VENUS - MESH ARCHITECTURE

2 files audited ● 2 files without findings

ID	Repo	File	SHA256 Checksum
VPG	VenusProtocol/vips	index.ts	2d364734b73c4704933eea1237f109073e77f0f65fec972403289de72c9a2d04
VBH	VenusProtocol/vips	index.ts	f17fb3dc164ea24220ecf304daaa55f88ba02a2d7c2c3595b56f7b2ed312278c

APPROACH & METHODS | VENUS - MESH ARCHITECTURE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Mesh Architecture 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.

REVIEW NOTES | VENUS - MESH ARCHITECTURE

This audit concerns the set-up of the mesh-architecture for the XVS token bridge. In particular, the audits focus was to determine any inconsistencies that may occur due to this change. The main difference between the current configuration and the mesh-architecture configuration is that it allows for destination to destination bridging and that it allows for multiple distinct paths from one chain to another.

A destination chain is any other chain than BSC, where XVS tokens must be minted when XVS is bridged to it and burned when XVS is bridged from it. As opposed to the BSC chain, which is the only source chain, where tokens are locked when they are bridged from it and are unlocked when tokens are bridged back to it. The total supply is preserved as each token on a destination chain must have a corresponding locked token on the source chain.

The configuration in scope will allow bridging ETH to/from opBNB, which are both destination chains. In addition, it will allow two separate paths to/from each currently supported chain, that is ETH, BSC, and opBNB. For example, to bridge tokens from ETH to BSC, a user can either bridge directly via the ETH/BSC bridge or can bridge via the ETH/opBNB bridge and then the opBNB/BSC bridge.

Bridging from a destination chain to another destination chain was considered in another audit titled **Venus - XVS Token Bridge** which can be found here: https://skynet.certik.com/projects/venus.

The commands that are in scope can be found here:

- https://github.com/VenusProtocol/vips/tree/a6a75f847746993c10a49ed97865c3a9162c71b4/multisig/proposals/ethereum/vip-016/index.ts
- https://github.com/VenusProtocol/vips/tree/2468c5ba5c1606f42a0536531a291dab53b91cc3/multisig/proposals/opbnbmainnet/vip-012/index.ts

The findings included are either relevant to the mesh-architecture or the values chosen for setup.

FINDINGS | VENUS - MESH ARCHITECTURE

3	0	0	0	0	3
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Mesh Architecture. Through this audit, we have uncovered 3 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
GLOBAL-01	Potential Implicit Whitelisting	Design Issue	Informational	Resolved
VBH-01	Send/Receive Limits Can Be Circumvented Via Different Paths	Logical Issue	Informational	Acknowledged
VPG-01	Same Send And Receive Limits May Cause Unexpected Behavior	Logical Issue	Informational	Resolved

GLOBAL-01 | POTENTIAL IMPLICIT WHITELISTING

Category	Severity	Location	Status
Design Issue	Informational		Resolved

Description

In order for an address to be whitelisted, they must be whitelisted on both the sending and receiving chain. With the mesh-architecture it allows for an address to be implicitly whitelisted between two chains. This may cause an issue if an address should not be whitelisted when transferring directly to/from a specific chain, but it is necessary to whitelist a path between the chains.

Note that this is a strictly hypothetical scenario and we are not aware of any protocols where such a scenario would cause an issues.

Scenario

Assume that `addressA` is whitelisted for direct bridging from ETH/BSC and from BSC/opBNB.

- Necessarily `addressA` is then whitelisted on ETH, BSC, and opBNB.
- However, this then implicitly whitelists `addressA` for direct bridging from `ETH/opBNB`.

Recommendation

We recommend considering the implicit whitelisting and ensure that it will not cause any potential issues with the intended whitelisted addresses.

Alleviation

`[Venus, 04/12/2024]`: "We have reviewed the whitelisted accounts, and we have added a couple of missed addresses in commit:

- a46cf94d7072726edee388d9cd6327a933dcaa17.

Regarding:

`In order for an address to be whitelisted, they must be whitelisted on both the sending and receiving chain`

We don't think this is mandatory. This is only true if the from/to addresses are the same. Otherwise (i.e. sending XVS from the Normal timelock on BNB Chain to the Venus Treasury contract on Ethereum), the addresses must be whitelisted only in

their networks. We think this reduces the chances to have implicit whitelistings (we are using different deployer wallets, to the deployed contracts have different addresses on each chain)"

`[CertiK, 04/16/2024]`: Considering that the client states they are using different addresses for each chain, we resolve the finding. However, we recommend considering implicit whitelisting in any future cases where the same address is whitelisted on multiple chains.

VBH-01 | SEND/RECEIVE LIMITS CAN BE CIRCUMVENTED VIA DIFFERENT PATHS

Category	Severity	Location	Status
Logical Issue	Informational	index.ts (base-opbnb): 6~9	Acknowledged

Description

The mapping `chainIdToMaxDailyLimit[dstChainId_]`, is designed to limit the maximum amount of XVS that can be bridged from the current chain to the chain with `dstChainId_` in a 24 hour period. Similarly, `chainIdToMaxDailyReceiveLimit[srcChainId_]` is designed to limit the maximum amount of XVS that can be bridged to the current chain from the chain with `srcChainId_` in a 24 hour period.

However, as there are now multiple paths between bridges, it is possible to bridge more than this amount. As such, this value represents the maximum amount that can be directly bridged, however, the actual amount that can be bridged is the sum of the maximum amounts that can bridged along all paths.

Scenario

Lets assume that we wish to bridge tokens from ETH to opBNB. Now, with the mesh architecture, there are two paths.

1. Bridge directly from ETH to opBNB.
2. Bridge from ETH to BSC and then bridge a second time from BSC to opBNB.

For simplicity assume that no XVS has been bridged during the current 24 hour period. The current setup will set the maximum daily receive limit on opBNB from ETH to be 50,000 and the maximum daily send limit on ETH to opBNB to be 50,000.

- A user uses multiple transactions to bridge 50,000 USD worth of XVS from ETH to opBNB using the direct ETH/opBNB bridge, reaching the maximum daily amount.
- To bridge more, the user then bridges 50,000 USD worth of XVS from ETH to BSC. (This can be done in a single transaction, as the single transaction limit is 100,000.)
- The user then bridges the 50,000 USD worth of XVS from BSC to opBNB in multiple transactions.

Thus a user is able to bridge 100,000 USD worth of XVS from ETH to opBNB.

Recommendation

We recommend setting the daily limits to account for the multiple paths.

Alleviation

`[Venus, 04/19/2024]`: "Our approach will involve refining and assessing bridge limits between two non-BNB chains, contingent upon the XVS liquidity of the source chain. Considering the existing limitations, there's no immediate need to adjust the values, given their already conservative nature."

VPG-01 | SAME SEND AND RECEIVE LIMITS MAY CAUSE UNEXPECTED BEHAVIOR

Category	Severity	Location	Status
Logical Issue	Informational	index.ts (base-ethereum): 6	Resolved

Description

Both contracts set the single send and receive limit to `10000`. Similarly, they set the max daily send and receive limits to be `50000`, where this value is determined by the USD value when the function is called.

As such tokens may be sent when the value of `XVS` dropped dramatically, so that when the message is to be received and the price recovers it will exceed the single receive limit or the max daily receive limit. Alternatively, the price of XVS may drop on one chains oracle, but remain constant on another chains oracle.

Scenario

Assume for simplicity that currently the price of 1 XVS is 1 USD.

- Assume that the price of XVS temporarily drops on the sending chain oracle, so that 1 XVS is .9 USD.
- A user then tries to bridge 11000 XVS, worth 9900 USD which is below the send limit.
- The send transaction of the bridge succeeds, however, before the receiving transaction is executed the price of XVS recovers to be 1 USD. Or alternatively, the oracle price on the receiving chain did not fluctuate in price and was consistently 1 USD.
- Thus on the receiving chain when `_isEligibleToReceive()` is called it will revert as the value of the tokens on the receiving chain is 11000 USD which exceeds the single transaction limit.

In this way, a user may be able to send an amount of XVS from one chain, but that will not be able to be received by another chain. If the price drop was only for a short time, then retrying a message may still revert requiring the tokens to be manually refunded.

Similarly, a temporary price drop can cause issues if it is sent to just reach the max daily receive limit for a chain. However, in this case it can be retried in the next 24 hour period.

Recommendation

We recommend considering adjusting the single send and receive limits, so that the send limit is slightly lower than the receive limit. Alternatively, we recommend warning users that if they choose a value of XVS that is close to the send limits, their transaction is at risk of not being executable on the receiving chain and may require them to retry during the next 24 hour period, or in the worst case, require manual intervention.

Alleviation

`[Venus, 04/12/2024]`: "The official Venus app applies a 10% margin on the limits configured to the contracts, and doesn't allow users to transfer more than that. For example, nowadays the single transfer limit is 100K according to the contracts, and the UI doesn't allow to transfer more than 90K

UI: https://app.venus.io/#/bridge?chainId=56"

`[CertiK, 04/16/2024]`: Given that the Venus team already makes this kind of consideration in their front end, we resolve the finding. We recommend users interact directly with the Venus UI, or else use a similar method in their own use.

APPENDIX | VENUS - MESH ARCHITECTURE

Finding Categories

Categories	Description
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
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.