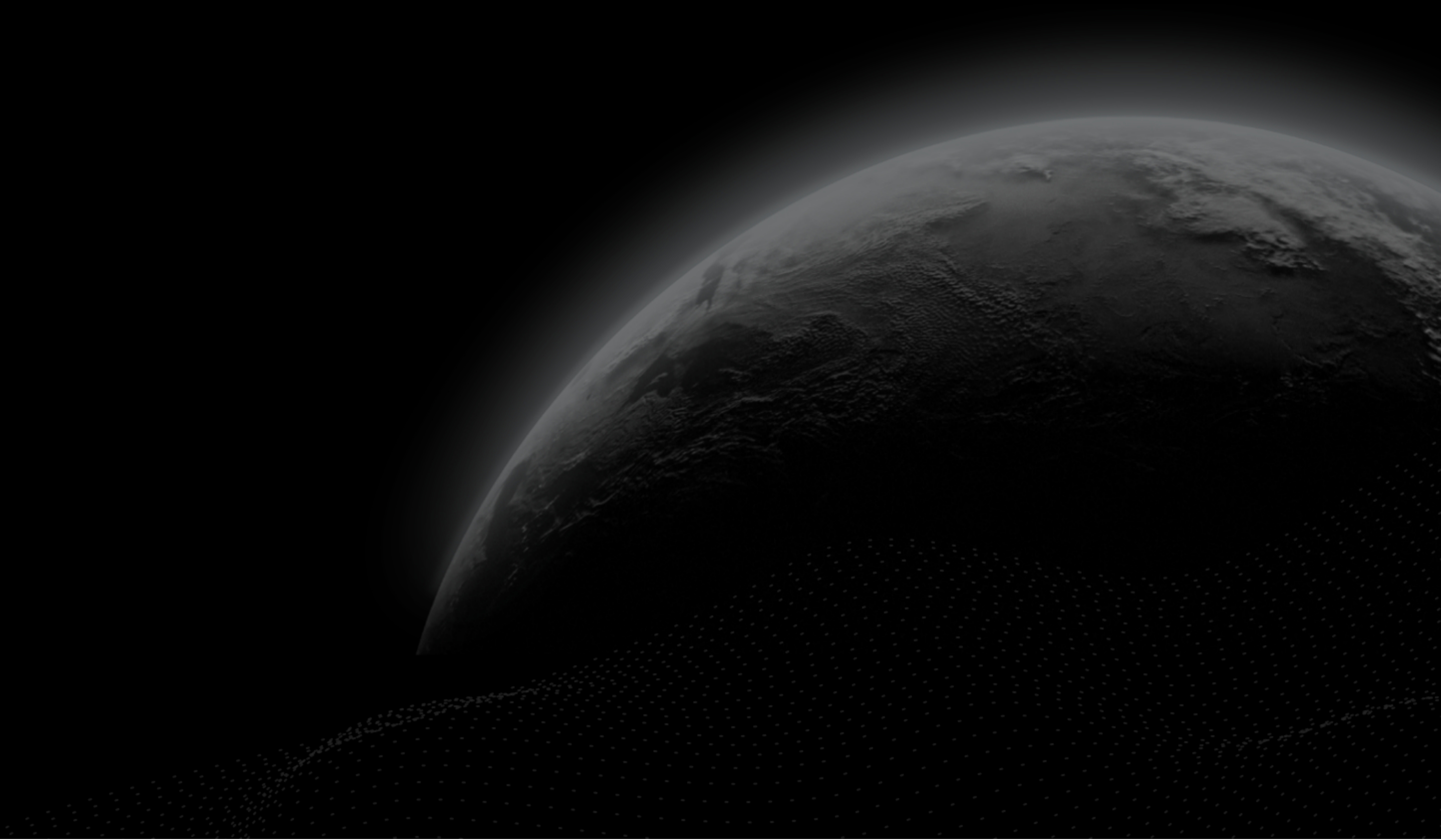
Security Assessment

Venus - VBNBAdmin

CertiK Assessed on Jul 17th, 2024



CertiK Assessed on Jul 17th, 2024

Venus - VBNBAdmin

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 07/17/2024	N/A

CODEBASE

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

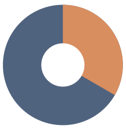
View All in Codebase Page

COMMITS

base: d89969ae25a6715016af56d62cc4a55d773d19a8

View All in Codebase Page

Vulnerability Summary



Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined
3	1	0	0	2	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.
🟧	1	Major	1 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.
🟨	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.
🟦	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 - VBNBADMIN

CODEBASE | VENUS - VBNBADMIN

Repository

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

Commit

base: d89969ae25a6715016af56d62cc4a55d773d19a8

AUDIT SCOPE | VENUS - VBNBADMIN

2 files audited ● 1 file with Acknowledged findings ● 1 file without findings

ID	Repo	File	SHA256 Checksum
● VBN	VenusProtocol/venus-protocol	contracts/Admin/VBNBAdmin.sol	8646ac74183004ac356cfbe1c36a178d404381cbdf7ead8ce088ed483c8bf529
● VBB	VenusProtocol/venus-protocol	contracts/Admin/VBNBAdminStorage.sol	58a549e3f8d64bef479ff79ccf9e55ccc8994d7a4a0d4f9f4f0d5971a7a7abf3

APPROACH & METHODS | VENUS - VBNBADMIN

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - VBNBAdmin 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 - VBNBADMIN

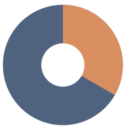
This audit concerns the changes made in PR-487.

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 to 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.

In particular, this PR is for the inclusion of the function `setInterestRateModel()` within contract `VBNBAdmin` , which acts as the admin role for the `VBNB` contract at address 0xA07c5b74C9B40447a954e1466938b865b6BBea36. The proxy acting as the `VBNBAdmin` can be found at address 0x9A7890534d9d91d473F28cB97962d176e2B65f1d and at the time of the audit, the current implementation of this proxy contract can be found at address 0x8c15384f1346bd977a689c0c51bd369e8d7313ca.

Note that contract `VBNB` is not upgradeable, but the contract `VBNBAdmin` is upgradeable. Previously, the function `setInterestRateModel()` did not exist within the `VBNBAdmin` contract, limiting the ability to call function `_setInterestRateModel()` within the `VBNB` contract. Including this function in the upgrade of `VBNBAdmin` provides the ability to call this function within `VBNB` and change the interest rate model used within the token contract.

FINDINGS | VENUS - VBNBADMIN



3	0	1	0	0	2
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - VBNBAdmin. 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
VBN-03	**Centralization Related Risks**	**Centralization**	**Major**	● **Acknowledged**
VBN-01	Potential Update To Unknown `InterestRateModel`	Design Issue	Informational	● Resolved
VBN-02	Type Inconsistency Between `VTokenInterface` Contracts Used	Inconsistency	Informational	● Acknowledged

VBN-03 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	● **Major**	**contracts/Admin/VBNBAdmin.sol: 99**	● **Acknowledged**

Description

Note that any centralization risks present in the existing codebase before the PR's in scope of this audit were not considered. Only those added to the in-scope PRs are addressed. 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.

In the contract `VBNBAdmin` the role the `DEFAULT_ADMIN_ROLE` of the `AccessControlManager` can grant addresses the privilege to call the function `setInterestRateModel()` .

Any compromise to the `DEFAULT_ADMIN_ROLE` or accounts granted this privilege may allow the hacker to take advantage of this authority and do set the interest rate model to a malicious contract to return borrow or supply rates that are higher or lower than expected.

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, 07/15/2024]` Regarding the DEFAULT_ADMIN_ROLE, we'll use the AccessControlManager (ACM) deployed at https://bscscan.com/address/0x4788629abc6cfca10f9f969efdeaa1cf70c23555. In this ACM, only 0x939bd8d64c0a9583a7dcea9933f7b21697ab6396 (Normal Timelock) has the DEFAULT_ADMIN_ROLE. And this contract is a Timelock contract used during the Venus Improvement Proposals. We'll allow Normal, Fast-track and Critical timelock contracts to execute the mentioned function (setInterestRateModel()).

Current config for the three Timelock contracts:

Normal: 24 hours voting + 48 hours delay Fast-track: 24 hours voting + 6 hours delay Critical: 6 hours voting + 1 hour delay

Addresses of the Timelock contracts:

Normal timelock: https://bscscan.com/address/0x939bD8d64c0A9583A7Dcea9933f7b21697ab6396 Fast-track timelock: https://bscscan.com/address/0x555ba73dB1b006F3f2C7dB7126d6e4343aDBce02 Critical timelock: https://bscscan.com/address/0x213c446ec11e45b15a6E29C1C1b402B8897f606d

--

We have been working on the VIP to upgrade the VBNBAdmin implementation and grant permissions. You can check the commands to be executed in that VIP here: https://github.com/VenusProtocol/vips/pull/297/files#diff-0b2889a429701394ce3daae7f9ef0b3dea44e2c71306a20d49c5da05462fdc08 (file bscmainnet.ts in the `vips` folder)

`[CertiK, 06/17/2024]` : Currently the setup described and to be implemented via the VIP will meet our mitigation standards. We can mark this finding as *Mitigated* after the deployment and setup when this can be verified on chain.

VBN-01 | POTENTIAL UPDATE TO UNKNOWN `InterestRateModel`

Category	Severity	Location	Status
Design Issue	● Informational	contracts/Admin/VBNBAdmin.sol: 99~100	● Resolved

Description

The function `setInterestRateModel()` was added to upgradeable contract logic for `VBNBAdmin` in order to make changes to the `interestRateModel` used in the `VBNB` contract at address 0xA07c5b74C9B40447a954e1466938b865b6BBea36 in the case where it is needed.

It is noted that the addition of this function in `VBNBAdmin` now provides the centralized authority with the ability to change the interest rate model of the `VBNB` contract to any interest rate model, including models that have not been reviewed or vetted previously.

Recommendation

We recommend only updating the interest rate model of the `VBNB` contract to interest rate models which have been thoroughly vetted and which are known to be compatible with the logic and configuration of the `VBNB` contract.

Alleviation

`[Venus, 07/17/2024]` : "We will be updating the IR using VIP (via Governance) so contracts will be reviewed and the Venus community will take care of it when updating."

VBN-02 TYPE INCONSISTENCY BETWEEN `VTokenInterface` CONTRACTS USED

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/Admin/VBNBAdmin.sol: 101~102	● Acknowledged

Description

Newly added function `setInterestRateModel()` in contract `VBNBAdmin` uses the following interface to interact with the `_setInterestRateModel()` function in the `VBNB` contract:

```
interface VTokenInterface {
    function _reduceReserves(uint reduceAmount) external returns (uint);

    function _acceptAdmin() external returns (uint);

    function comptroller() external returns (address);

    function _setInterestRateModel(address newInterestRateModel) external returns
(uint);
}
```

However, the `VTokenInterface` used in the `VBNB` contract at address 0xA07c5b74C9B40447a954e1466938b865b6BBea36 declares the function `_setInterestRateModel()` in the following way, using the type `InterestRateModel` rather than type `address` for the input.

```
  function _setInterestRateModel(InterestRateModel newInterestRateModel) public
returns (uint);
```

Recommendation

We recommend correcting the inconsistency between interfaces as a best practice in keeping formatting the same across contracts.

Alleviation

`[Venus, 07/15/2024]`: "The InterestRateModel contract uses a different solidity version (^0.5.16) compared to vBNBAdmin contract (0.8.25). Therefore we cannot use InterestRateModel in the new _setInterestRateModel function added to VTokenInterface"

APPENDIX | VENUS - VBNBADMIN

Finding Categories

Categories	Description
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
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.