Venus - BNB Blockrate Increase

Security Assessment

CertiK Assessed on Apr 17th, 2025

CertiK Assessed on Apr 17th, 2025

Venus - BNB Blockrate Increase

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

Executive Summary

TYPES
Lending

ECOSYSTEM
Binance Smart Chain (BSC)

METHODS
Manual Review, Static Analysis

LANGUAGE
Solidity

TIMELINE
Delivered on 04/17/2025

KEY COMPONENTS
N/A

CODEBASE
https://github.com/VenusProtocol/venus-protocol
https://github.com/VenusProtocol/governance-contracts
https://github.com/VenusProtocol/solidity-utilities
View All in Codebase Page

COMMITS
Base PR-576: 1824cb532eda6567fc2507256f0cd0ef26543e87
Base PR-139: 851faecda4287738f68a416cea7fbc63c0006909
Base PR-574: 0859174eb79e773e3a00c7fd6b20330766efa7ea
View All in Codebase Page

Vulnerability Summary

4	3	0	1	0
Total Findings	Resolved	Partially Resolved	Acknowledged	Declined

1	Centralization	1 Acknowledged	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.
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	2 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 - BNB BLOCKRATE INCREASE

CODEBASE | VENUS - BNB BLOCKRATE INCREASE

Repository

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

https://github.com/VenusProtocol/governance-contracts

https://github.com/VenusProtocol/solidity-utilities

Commit

Base PR-576: 1824cb532eda6567fc2507256f0cd0ef26543e87
Base PR-139: 851faecda4287738f68a416cea7fbc63c0006909
Base PR-574: 0859174eb79e773e3a00c7fd6b20330766efa7ea
Base PR-32: 7bfd8c9e7e3db4b4deb0333658e985a2815888ed
Update 1 PR-576 7cadd2085a53183dc3356592c82d3bb4dce3c91e
Update 1 PR-139: c775484fa74a23eb66302507ee1214676c9f7aaa
Update1 PR-574: c3b102fc8cc6c55e5a3545d43354f940df71606a
Update 1 PR-32: 90b9a61d3ddcd9e6e2595c1964f63ee5a5132645

AUDIT SCOPE | VENUS - BNB BLOCKRATE INCREASE

6 files audited ● 6 files without findings

ID	Repo	File	SHA256 Checksum
TMV	VenusProtocol/solidity-utilities	TimeManagerV5.sol	657363dac5b8469079b0e7061f3bf711b699aae625a9912e648731c1ec261ebc
VAI	VenusProtocol/venus-protocol	VAIController.sol	1f298596b11e2638588e6ceedd77a03f4d7c8bdad1d3df6ffb428497d6810c80
XVS	VenusProtocol/venus-protocol	XVSVault.sol	ffc92d59cce3f90e323c01ee5be77905c82d2c0c2cf06fb1e5fb17e26aaac9cd
CVU	VenusProtocol/venus-protocol	CheckpointView.sol	7ddc338bdbda17c30e814556ed82fc9c6079080f62d4ce040b18873dea9ba787
GBD	VenusProtocol/governance-contracts	GovernorBravoDelegate.sol	44e006e895c4cd49983946b427e596e8ba109103ac3e80bf4ede0ac2468881ac
GBI	VenusProtocol/governance-contracts	GovernorBravoInterfaces.sol	b9e3602fb4ce996f7a1994367ab56864f7a5168af7de2d62fdb9368fa5b6db3d

APPROACH & METHODS | VENUS - BNB BLOCKRATE INCREASE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - BNB Blockrate Increase 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 - BNB BLOCKRATE INCREASE

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

- PR-32
- PR-574
- PR-139
- PR-576

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.

The audit only concerned the changes in the PRs mentioned above. The protocol may depend on block times in other places that those in the PR (for example reward distributor speeds), however, they were not considered during the audit.

The main motivation behind these PRs are to make necessary changes due to the scheduled changing of block times for BSC and opBNB. BSC plans to adjust the blocktime from 3 seconds to 1.5 seconds (source) and then in a later phase from 1.5 seconds to 0.75 seconds (source). opBNB plans to adjust the blocktime from 1 second to 0.5 seconds (source).

PR-32

Adds an internal setter function `_setBlocksPerYear()` to the `TimeManagerV5` contract. This is to enable contracts that inherit the `TimeManagerV5` to add setter functions to adjust the amount of blocks per year to adjust for the scheduled changes.

PR-574

Updates `getBlocksPerYear()` in the `VAIController` contract to assume that blocks are 1.5 seconds as opposed to 3 seconds. It also adds a setter function `setBlocksPerYear()` to the `XVSVault` contract in order to allow the amount of blocks per year to be changed. This is done by utilizing the internal setter function `_setBlocksPerYear()` added to the `TimeManagerV5` contract, which it inherits.

PR-139

Updates the `GovernorBravoDelegate` contract by making the min voting period, max voting period, min voting delay, and max voting delay configurable via the function `setValidationParams()`, which is only callable by the admin. Similarly, it adds a function `setProposalConfigs()`, only callable by the admin, that allows the proposal configurations to be updated. This allows for the validation parameters and the proposal configurations to be adjusted based on the new block times as the voting period and voting delay are given by an amount of blocks.

PR-576

Adds the `CheckpointView` contract which is designed to make static calls via the fallback function to one of two stored addresses depending on if it is before or after a `CHECKPOINT_TIMESTAMP`. In particular, this contract is designed to be used for interest rate models where the blocks per year must be adjusted. The two rate models for the differing blocks per year can be set as the two stored addresses and the time of the block time change can be set as the timestamp.

FINDINGS | VENUS - BNB BLOCKRATE INCREASE

4	0	1	0	0	1	2
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - BNB Blockrate Increase. Through this audit, we have uncovered 4 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
VBB-04	**Centralization Related Risks**	**Centralization**	**Centralization**	**Acknowledged**
VBB-01	Missing Input Validation	Logical Issue	Minor	Resolved
VBB-02	Missing And Incomplete Natspec Comments	Inconsistency	Informational	Resolved
VBB-03	Typos And Inconsistencies	Inconsistency	Informational	Resolved

VBB-04 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	Centralization	GovernorBravoDelegate.sol (Base PR-139 GovernorBravoDelegate): 138~139, 162~163; XVSVault.sol (Base PR-574 XVSVault): 918~919	Acknowledged

Description

Note that the scope of the audit did not concern any existing centralization risks and only considers those added in the in scope PRs.

In the contract `GovernorBravoDelegate`, the role `admin` has authority over the following added functions:

- `setValidationParams()`
- `setProposalConfigs()`

Any compromise to the `admin` account may allow a hacker to take advantage of this authority and do the following:

- Set new validation parameters to allow proposals to be configured with voting periods or delays that are much smaller or larger than expected.
- Update proposal configurations withing the validation parameters so that the voting delay, period, and proposal threshold are not as expected.

In the contract `XVSVault` the role `DEFAULT_ADMIN_ROLE` of the `AccessControlManager` can grant addresses the privilege to call the added function:

- `setBlocksPerYear()`

Any compromise to the `DEFAULT_ADMIN_ROLE` of the `AccessControlManager` may allow a hacker to take advantage of this authority and do the following:

- Update the amount of blocks per year to more or less than the actual amount of blocks per year.

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, 04/17/2025]`: "Nowadays, admin is a multisig wallet, but it will be transferred to the Venus Normal Timelock on BNB Chain (0x939bD8d64c0A9583A7Dcea9933f7b21697ab6396). So, the functions `setValidationParams()` and `setProposalConfigs()` will be only executable via Governance.

On BNB chain, we'll use the AccessControlManager (ACM) deployed at 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."

`[CertiK, 04/17/2025]`: Provided the steps outline above are taken, we would consider this finding *Mitgated*. However, until these actions are taken so that we can verify them on chain, we mark this finding as *Acknowleged*.

VBB-01 | MISSING INPUT VALIDATION

Category	Severity	Location	Status
Logical Issue	Minor	GovernorBravoDelegate.sol (Base PR-139 GovernorBravoDelegate): 138, 162, 164~170; TimeManagerV5.sol (Base PR-32): 67; CheckpointView.sol (Base PR-576): 28, 31~32	Resolved

Description

In the contract `CheckpointView`:

- The input `checkpointTimestamp` is not checked to be in the future. If the current `block.timestamp` is greater than or equal to the input `checkpointTimestamp`, then it will always use `DATA_SOURCE_2` so that the use of the contract is unnecessary.
- The input `dataSource1` and `dataSource2` are not checked to be different. If `dataSource1` and `dataSource2` are the same address, then the contract will always use the same data source making the use of the contract unnecessary.

In the contract `GovernorBravoDelegate`:

- The function `setValidationParams()` does not check that the `minVotingPeriod < maxVotingPeriod` and that the `minVotingDelay < maxVotingDelay`. If the max values are set lower than the min values then it can prevent proposal configurations from being set. Note that if this is added then the check in the function `setProposalConfigs()` for if the validation params are set can be simplified.
- The function `setProposalConfigs()` does not check that the input `proposalConfigs_` length. This allows `setProposalConfigs()` to be called with an input array whose length is larger than 3 so that it will set a configuration for a proposal type that is not defined. Note that it should be determined if `setProposalConfigs()` should always set all proposal configs and if not consider refactoring the code to allow for it to set individual proposal configurations.

In the contract `TimeManagerV5`:

- The function `_setBlocksPerYear` does not make any validations on the input `blocksPerYear_` except to ensure it is nonzero. This allows it to be set to an arbitrary nonzero value. We recommend considering adding a minimum and maximum value to validate against.

Recommendation

We recommend adding the input validations mentioned above.

Alleviation

`[CertiK, 04/17/2025]`: The client made the recommended changes for `GovernorBravoDelegate` in commits

- 2b5f2439eb003fb129816f78b06026bf4f6254c3;
- c775484fa74a23eb66302507ee1214676c9f7aaa.

For the other contracts and input validations the client stated the prefer to not add any extra checks and instead will rely on them to be checked during the governance process.

VBB-02 | MISSING AND INCOMPLETE NATSPEC COMMENTS

Category	Severity	Location	Status
Inconsistency	Informational	GovernorBravoInterfaces.sol (Base PR-139 GovernorBravoInterfaces): 224; CheckpointView.sol (Base PR-576): 36~39	Resolved

Description

In the contract `CheckpointView`:

- The NatSpec comments for the `fallback()` function does not include the return value.

In the file `GovernorBravoInterfaces`:

- There are no NatSpec comments above the `GovernorBravoDelegateStorageV3` contract.

Recommendation

We recommend adding the missing NatSpec comments mentioned above.

Alleviation

`[CertiK, 04/17/2025]`: The client made the recommended changes in commits

- 9ac549e43740243899f66d3a16c09f51a3b094c2;
- 7cadd2085a53183dc3356592c82d3bb4dce3c91e.

VBB-03 | TYPOS AND INCONSISTENCIES

Category	Severity	Location	Status
Inconsistency	Informational	TimeManagerV5.sol (Base PR-32): 27, 28, 31; XVSVault.sol (Base PR-574 XVSVault): 915	Resolved

Description

In the contract `TimeManagerV5`:

- In the event `InitializeTimeManager`, `timebased` is not in camel case.
- In the event `SetBlocksPerYear`, `prevBlocksPeryear` is not in camel case.

In the contract `XVSVault`:

- The `@notice` comment does not follow the conventions of the other `@notice` comments in the contract.

Recommendation

We recommend fixing the typos and inconsistencies mentioned above.

Alleviation

`[CertiK, 04/17/2025]`: The client made some of the recommended changes in commits:

- 90b9a61d3ddcd9e6e2595c1964f63ee5a5132645;
- c3b102fc8cc6c55e5a3545d43354f940df71606a.

The client opted to not make the recommended changes for `timebased` stating that they already use this event on mainnet.

APPENDIX | VENUS - BNB BLOCKRATE INCREASE

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.
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.

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.

Elevating Your Entire Web3 Journey

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.