Interest Rate Models - Venus

Executive Summary

This audit report was prepared by Quantstamp, the leader in blockchain security.

Type	DeFi Lending Protocol
Timeline	2024-08-12 through 2024-08-13
Language	Solidity
Methods	Architecture Review, Unit Testing, Functional Testing, Computer-Aided Verification, Manual Review
Specification	Two Kinks Interest Rate - Audit scope Isolated Pools README Venus Protocol README
Source Code	• VenusProtocol/venus-protocol #25475d0 • VenusProtocol/isolated-pools #37ffc79
Auditors	• Cameron Biniamow Auditing Engineer • Ibrahim Abouzied Auditing Engineer • Jennifer Wu Auditing Engineer

Documentation quality	High
Test quality	Medium
Total Findings	1 Acknowledged: 1
High severity findings	0
Medium severity findings	0
Low severity findings	0
Undetermined severity findings	0
Informational findings	1 Acknowledged: 1

Summary of Findings

Quantstamp audited the Two Kinks Interest Rate implementation for the Venus Protocol's Core and Isolated pools. The in-scope files were included in two separate repositories, one for the Core pool and the other for the Isolated pools; however, the majority of the Two Kinks Interest Rate logic is identical between the two repositories. Only the Two Kinks Interest Rate contracts in both repositories were in scope for this audit. Users should refer to previous Venus audits that cover how an Interest Rate contract may integrate with the rest of the system.

The new interest rate model is an upgrade from a Single-Kink to a Two-Kink structure, introducing a second point where the interest rate slope changes as utilization increases. This Two-Kink model allows for distinct base interest rates and varying slopes across the utilization intervals `[0, KINK_1)`, `[KINK_1, KINK_2)`, and `[KINK_2, 100]`.

During the review, the audit team discovered high-quality code and documentation in the Venus Protocol codebases, streamlining the audit process significantly. The codebases included test suites that produced moderate to high code coverage. Due to lower-than-recommended branch and function coverage, the audit team suggests improving the test suites to increase code coverage to over 90%.

No notable issues were identified during the audit; however, this report includes an informational issue regarding a possible decreasing supply rate under the right conditions. Additionally, two auditor suggestions are listed to ensure adherence to best practices.

Update: The Venus team fixed or acknowledged all issues listed in this report.

ID	DESCRIPTION	SEVERITY	STATUS
VEN-1	**Decreasing Supply Interest Rate**	● Informational	Acknowledged

Assessment Breakdown

Quantstamp's objective was to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices.

> **Disclaimer**
> Only features that are contained within the repositories at the commit hashes specified on the front page of the report are within the scope of the audit and fix review. All features added in future revisions of the code are excluded from consideration in this report.

Possible issues we looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Mishandled exceptions and call stack limits
- Unsafe external calls
- Integer overflow / underflow
- Number rounding errors
- Reentrancy and cross-function vulnerabilities
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

Methodology

1. Code review that includes the following
    1. Review of the specifications, sources, and instructions provided to Quantstamp to make sure we understand the size, scope, and functionality of the smart contract.
    2. Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
    3. Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Quantstamp describe.
2. Testing and automated analysis that includes the following:
    1. Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
    2. Symbolic execution, which is analyzing a program to determine what inputs cause each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarity, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, and actionable recommendations to help you take steps to secure your smart contracts.

Scope

The scope of this audit is strictly limited to the files listed below. All files not explicitly listed are considered out of scope and were not reviewed during the audit. Since only the interest rate model contracts were in scope, any interactions with the interest rate model contracts from other contracts in the codebase were not reviewed.

Files Included

- **https://github.com/VenusProtocol/venus-protocol**
    - `contracts/InterestRateModels/InterestRateModelV8.sol`
    - `contracts/InterestRateModels/TwoKinksInterestRateModel.sol`
- **https://github.com/VenusProtocol/isolated-pools**
    - `contracts/TwoKinksInterestRateModel.sol`

Operational Considerations

The `TwoKinksInterestRateModel.sol` contract in the `venus-protocol` repository is designed to operate on the BNB chain, which has a constant block time of three seconds. Using this contract on chains without constant block times or chains with block times deviating from three seconds will result in unexpected behavior.

Key Actors And Their Capabilities

The `TwoKinksInterestRateModel.sol` contracts in both repositories only contain immutable state variables and read-only functions. Therefore, the deployer or any other protocol key actor does not retain privileged capabilities following contract deployment.

Findings

VEN-1 Decreasing Supply Interest Rate

● Informational ⓘ Acknowledged

Update

The client acknowledged the issue and provided the following explanation:

```
We will simulate the interest rate model parameters before enabling it. Any change in the risk
parameters requires the Community's approval (via Governance), so, apart from the simulation, the
Community will be able to review the suggested change
```

File(s) affected: `isolated-pools/contracts/TwoKinksInterestRateModel.sol` , `venus-protocol/contracts/InterestRateModels/TwoKinksInterestRateModel.sol`

Description: In the proposed interest rate model, improper calibration of the multipliers, particularly between `KINK1` and `KINK2` , can result in unintended consequences where the borrowing rate decreases as utilization increases and the supply rate decreases as utilization rises. This behavior is undesirable as it can disrupt market incentives, leading to reduced participation by lenders and borrowers, and potentially destabilizing the lending protocol.

Recommendation: Before deploying the model, the interest rate model parameters should be simulated. The supply rate should increase as the utilization rate increases; otherwise, a negative feedback cycle can occur.

Auditor Suggestions

VEN-S2 Use of Immutable Variables for Precomputed Constants

Fixed

Update

The client fixed the issue in commits `cf5b5287559b12841339f322de4478f9a4757783` , `499a6bb3f52ef6df174f1e5f4bec51455801227f` and provided the following explanation:

```
Immutable variables RATE_1 and RATE_2 added, as suggested
```

File(s) affected: `isolated-pools/contracts/TwoKinksInterestRateModel.sol` , `venus-protocol/contracts/InterestRateModels/TwoKinksInterestRateModel.sol`

Description: The contracts calculate maximum kink interest rate values `rate1` and `rate2` during each `_getBorrowRate` function call. The maximum rates are based on constants (`KINK_1` , `MULTIPLIER_PER_BLOCK_OR_SECOND` , `BASE_RATE_PER_BLOCK_OR_SECOND` , etc.) that are not dependent on `util` . Since every call recomputes these values, additional gas is consumed.

Recommendation: Precompute and store the maximum kink rate values (`rate1` , `rate2`) from the function `_getBorrowRate` as `immutable` variables during the contract's deployment.

VEN-S3 Document the Scale of Contract State Variables

Fixed

Update

The client fixed the issue in commits `ae53d56ba0fa2a05c3c5605b8d9f48703fbcc775` , `2044826425fbf80d1e6877741c260c49707a68f6` and provided the following explanation:

```
We added the scale of the variables in the comments, as suggested
```

File(s) affected: `isolated-pools/contracts/TwoKinksInterestRateModel.sol` , `venus-protocol/contracts/InterestRateModels/TwoKinksInterestRateModel.sol`

Description: Document the scale of all contract state variables to improve code comprehension.

Recommendation: Add code comments stating the scale of the state variable (e.g., "scaled by EXP_SCALE").

Definitions

- **High severity** – High-severity issues usually put a large number of users' sensitive information at risk, or are reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.
- **Medium severity** – Medium-severity issues tend to put a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or are reasonably likely to lead to moderate financial impact.
- **Low severity** – The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.
- **Informational** – The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.
- **Undetermined** – The impact of the issue is uncertain.
- **Fixed** – Adjusted program implementation, requirements or constraints to eliminate the risk.
- **Mitigated** – Implemented actions to minimize the impact or likelihood of the risk.
- **Acknowledged** – The issue remains in the code but is a result of an intentional business or design decision. As such, it is supposed to be addressed outside the programmatic means, such as: 1) comments, documentation, README, FAQ; 2) business processes; 3) analyses showing that the issue shall have no negative consequences in practice (e.g., gas analysis, deployment settings).

Appendix

File Signatures

The following are the SHA-256 hashes of the reviewed files. A file with a different SHA-256 hash has been modified, intentionally or otherwise, after the security review. You are cautioned that a different SHA-256 hash could be (but is not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of the review.

Files

- `ed2...5f9 ./isolated-pools/contracts/TwoKinksInterestRateModel.sol`
- `e3b...855 ./venus-protocol/contracts/InterestRateModels/TwoKinksInterestRateModel.sol`
- `e3b...855 ./venus-protocol/contracts/InterestRateModels/InterestRateModelV8.sol`

Tests

- `954...073 ./isolated-pools/tests/hardhat/TwoKinksInterestRateModel.ts`
- `abc...6e6 ./venus-protocol/tests/hardhat/InterestRateModels/TwoKinksInterestRateModel.ts`

Toolset

The notes below outline the setup and steps performed in the process of this audit.

Setup

Tool Setup:

- Slither v0.10.2

Steps taken to run the tools:

1. Install the Slither tool: `pip3 install slither-analyzer`
2. Run Slither from the project directory: `slither .`

Automated Analysis

Slither

We have executed Slither, filtered the reported issues, and incorporated the valid ones into the report. Please note that only issues related to the scope of the audit are reported.

Test Suite Results

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

The test suite was executed by running the following command:

- `npx hardhat coverage --testfiles "tests/hardhat/InterestRateModels/*"`

All seven tests were run successfully.

```
  Two Kinks Interest Rate Model Tests
    ✔ Utilization rate: borrows is zero
    ✔ Utilization rate
    ✔ Borrow Rate: below kink1 utilization
    ✔ Borrow Rate: above kink1 and below kink2 utilization (48ms)
    ✔ Borrow Rate: above kink2 utilization (46ms)
    ✔ Borrow Rate: above kink2 utilization and negative multipliers (134ms)
    ✔ Supply Rate


  7 passing (537ms)
```

https://github.com/VenusProtocol/isolated-pools

The test suite was executed by running the following command:

- `npx hardhat coverage --testfiles "tests/hardhat/TwoKinksInterestRateModel.ts"`

All 16 tests were run successfully.

```
  Two Kinks Interest Rate Model Tests
    ✔ Utilization rate: borrows and badDebt is zero
    ✔ Should return correct number of blocks
    ✔ Utilization rate
    ✔ Borrow Rate: below kink1 utilization
    ✔ Borrow Rate: above kink1 and below kink2 utilization (49ms)
    ✔ Borrow Rate: above kink2 utilization (51ms)
    ✔ Borrow Rate: above kink2 utilization and negative multipliers (172ms)
    ✔ Supply Rate

  TimeBased Two Kinks Interest Rate Model Tests
    ✔ Utilization rate: borrows and badDebt is zero
    ✔ Should return correct number of blocks
    ✔ Utilization rate
    ✔ Borrow Rate: below kink1 utilization
    ✔ Borrow Rate: above kink1 and below kink2 utilization (74ms)
    ✔ Borrow Rate: above kink2 utilization (66ms)
    ✔ Borrow Rate: above kink2 utilization and negative multipliers (132ms)
    ✔ Supply Rate


  16 passing (1s)
```

Code Coverage

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

Code coverage was obtained by running the following command:

- `npx hardhat coverage --testfiles "tests/hardhat/InterestRateModels/*"`

The test suite produced moderate code coverage; however, branch coverage is lower than recommended. Consider improving the test suite to increase branch coverage to over 90%.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/InterestRateModels/	100	56.25	100	93.18	
InterestRateModelV8.sol	100	100	100	100	
TwoKinksInterestRateModel.sol	100	56.25	100	93.18	88,92,151
All files	100	56.25	100	93.18	

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines

https://github.com/VenusProtocol/isolated-pools

Code coverage was obtained by running the following command:

- `npx hardhat coverage --testfiles "tests/hardhat/TwoKinksInterestRateModel.ts"`

The test suite produced moderate code coverage; however, branch and function coverage is lower than recommended. Consider improving the test suite to increase branch and function coverage to over 90%.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/	96.97	56.25	85.71	91.67	
InterestRateModel.sol	0	100	0	0	46
TwoKinksInterestRateModel.sol	100	56.25	100	93.62	89,93,169
All files	96.97	56.25	85.71	91.67	

Changelog

- 2024-08-14 - Initial report
- 2024-08-19 - Final report

About Quantstamp

Quantstamp is a global leader in blockchain security. Founded in 2017, Quantstamp's mission is to securely onboard the next billion users to Web3 through its best-in-class Web3 security products and services.

Quantstamp's team consists of cybersecurity experts hailing from globally recognized organizations including Microsoft, AWS, BMW, Meta, and the Ethereum Foundation. Quantstamp engineers hold PhDs or advanced computer science degrees, with decades of combined experience in formal verification, static analysis, blockchain audits, penetration testing, and original leading-edge research.

To date, Quantstamp has performed more than 500 audits and secured over $200 billion in digital asset risk from hackers. Quantstamp has worked with a diverse range of customers, including startups, category leaders and financial institutions. Brands that Quantstamp has worked with include Ethereum 2.0, Binance, Visa, PayPal, Polygon, Avalanche, Curve, Solana, Compound, Lido, MakerDAO, Arbitrum, OpenSea and the World Economic Forum.

Quantstamp's collaborations and partnerships showcase our commitment to world-class research, development and security. We're honored to work with some of the top names in the industry and proud to secure the future of web3.

Notable Collaborations & Customers:

- Blockchains: Ethereum 2.0, Near, Flow, Avalanche, Solana, Cardano, Binance Smart Chain, Hedera Hashgraph, Tezos
- DeFi: Curve, Compound, Maker, Lido, Polygon, Arbitrum, SushiSwap
- NFT: OpenSea, Parallel, Dapper Labs, Decentraland, Sandbox, Axie Infinity, Illuvium, NBA Top Shot, Zora
- Academic institutions: National University of Singapore, MIT

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by Quantstamp; however, Quantstamp does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication or other making available of the report to you by Quantstamp.

Notice of confidentiality

This report, including the content, data, and underlying methodologies, are subject to the confidentiality and feedback provisions in your agreement with Quantstamp. These materials are not to be disclosed, extracted, copied, or distributed except to the extent expressly authorized by Quantstamp.

Links to other websites

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Quantstamp. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites&aspo; owners. You agree that Quantstamp are not responsible for the content or operation of such web sites, and that Quantstamp shall have no liability to you or any other person or entity for the use of third-party web sites. Except as described below, a hyperlink from this web site to another web site does not imply or mean that Quantstamp endorses the content on that web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the report. Quantstamp assumes no responsibility for the use of third-party software on any website and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any output generated by such software.

Disclaimer

The review and this report are provided on an as-is, where-is, and as-available basis. To the fullest extent permitted by law, Quantstamp disclaims all warranties, expressed implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. You agree that access and/or use of the report and other results of the review, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE. This report is based on the scope of materials and documentation provided for a limited review at the time provided. You acknowledge that Blockchain technology remains under development and is subject to unknown risks and flaws and, as such, the report may not be complete or inclusive of all vulnerabilities. The review is limited to the materials identified in the report and does not extend to the compiler layer, or any other areas beyond the programming language, or programming aspects that could present security risks. The report does not indicate the endorsement by Quantstamp of any particular project or team, nor guarantee its security, and and may not be represented as such. No third party is entitled to rely on the report in any any way, including for the purpose of making any decisions to buy or sell a product, product, service or any other asset. Quantstamp does not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party, or or any open source or third-party software, code, libraries, materials, or information to, to, called by, referenced by or accessible through the report, its content, or any related related services and products, any hyperlinked websites, or any other websites or mobile applications, and we will not be a party to or in any way be responsible for monitoring any any transaction between you and any third party. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

Quantstamp