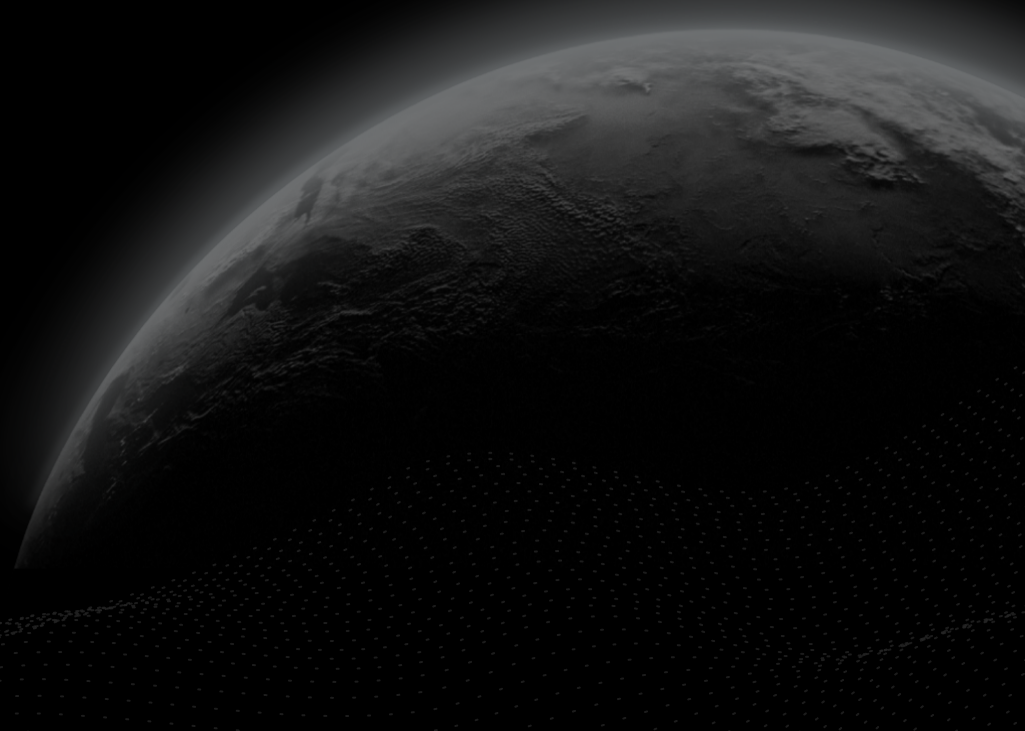
CERTIK

Security Assessment

Range Protocol

CertiK Verified on Apr 26th, 2023



CertiK Verified on Apr 26th, 2023

Range Protocol

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Other	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 04/26/2023	N/A

CODEBASE

https://github.com/Range-Protocol/contracts/

...View All

COMMITS

dea888b7c37f38ca8910d0b70979a752dd55ae1c

...View All

Vulnerability Summary

8	1	0	0	7	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

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.
1	Medium	1 Acknowledged	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
4	Minor	1 Resolved, 3 Acknowledged	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	3 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 | RANGE PROTOCOL

CODEBASE | RANGE PROTOCOL

Repository

https://github.com/Range-Protocol/contracts/

Commit

dea888b7c37f38ca8910d0b70979a752dd55ae1c

AUDIT SCOPE | RANGE PROTOCOL

4 files audited ● 3 files with Acknowledged findings ● 1 file without findings

ID	File	SHA256 Checksum
RPF	contracts/RangeProtocolFactory.sol	9e2d45b0d5bc0656ccb9c488b2cdb0824f0176d09729389f2b5905bef5d6a1d9
RPV	contracts/RangeProtocolVault.sol	169a3a73934bed6f2337a7874c19043937026bee598490c5de8dffbc62c77b41
RPS	contracts/RangeProtocolVaultStorage.sol	e09a1e72dd62b720c780a2426ee2c280f0f94460e521cee1e1c97c8b82ec47c4
ORP	contracts/abstract/Ownable.sol	081252774e673af772a8bec60b722d69cd5bfa3795ec39ad6a905dc26dfbbd7a

APPROACH & METHODS | RANGE PROTOCOL

This report has been prepared for Range Protocol to discover issues and vulnerabilities in the source code of the Range Protocol 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.

DECENTRALIZATION EFFORTS | RANGE PROTOCOL

Description

In the contract `Ownable` the role `_manager` has authority over the functions listed below. Any compromise to the `_manager` account may allow the hacker to take advantage of this authority.

- `transferOwnership()`
- `renounceOwnership()`

In the contract `RangeProtocolFactory` the role `_manager` has authority over the functions listed below. Any compromise to the `_manager` account may allow the hacker to take advantage of this authority.

- `createVault()`
- `upgradeVaults()`
- `upgradeVault()`

In the contract `RangeProtocolVault` the role `_manager` has authority over the functions listed below. Any compromise to the `_manager` account may allow the hacker to take advantage of this authority.

- `updateTicks()`
- `removeLiquidity()`
- `swap()`
- `addLiquidity()`
- `pullFeeFromPool()`
- `updateFees()`

In the contract `RangeProtocolVault` the role `factory` has authority over the functions listed below. Any compromise to the `factory` account may allow the hacker to take advantage of this authority.

- `_authorizeUpgrade()`

In the contract `RangeProtocolVault` the role `pool` has authority over the functions listed below. Any compromise to the `pool` account may allow the hacker to take advantage of this authority.

- `uniswapV3MintCallback()`
- `uniswapV3SwapCallback`

Upgradeable

In addition, RangeProtocolVault is an upgradeable contract, and the owner can upgrade the contract without the community's commitment. If an attacker compromises the account, the attacker can change the implementation of the contract and drain

tokens from the contract.

Recommendations

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.

FINDINGS | RANGE PROTOCOL

8	0	0	1	4	3
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Range Protocol . Through this audit, we have uncovered 8 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
RPV-01	Fees Can Be Transferred To Zero Address	Logical Issue, Control Flow	Medium	Acknowledged
RPB-02	Third-Party Dependencies	Volatile Code	Minor	Acknowledged
RPB-03	Incompatibility With Deflationary Tokens	Logical Issue	Minor	Acknowledged
RPV-03	Discussion On Ownerable Contract	Logical Issue	Minor	Resolved
RPV-04	Lack Of Return Value Handling	Volatile Code	Minor	Acknowledged
GLOBAL-02	Discussion On The Vault Manager Responsibilities	Business Model	Informational	Acknowledged
GLOBAL-04	Discussion On User Strategy	Business Model	Informational	Acknowledged
RPV-06	Wrong Fee Value Emitted	Data Flow	Informational	Acknowledged

RPV-01 | FEES CAN BE TRANSFERRED TO ZERO ADDRESS

Category	Severity	Location	Status
Logical Issue, Control Flow	Medium	contracts/RangeProtocolVault.sol: 405~406, 408~409	Acknowledged

Description

In the function `collectManager()`, the accumulated fees, including both performance fee and managing fee, will be transferred to the `_manager` address. Since the `renounceOwnership()` function is given in the `Ownerable` contract. If the ownership is renounced, the `_manager` address will be `address(0)`, and thus the tokens (`token0`, `token1` or both) will be locked in the zero address.

Furthermore, unlike the function `pullFeeFromPool()`, the `collectManager()` does not have the `onlyManager` modifier. All external users can freely call the `collectManager()` function, such that If the `_manager` is renounced, all users can call the function and lock the fees to the zero address.

Recommendation

Recommend adding the `onlyManager` modifier, such that when `_manager` is renounced, no one can call the `collectManager()` function.

Alleviation

[Range Team]:

We have restricted the function to be only called by the Vault manager. In case, if ownership is renounced by the manager then the factory owner can deploy a new implementation to rescue the funds through DAO vote.

RPB-02 | THIRD-PARTY DEPENDENCIES

Category	Severity	Location	Status
Volatile Code	Minor	contracts/RangeProtocolFactory.sol; contracts/RangeProtocolVault.sol; contracts/RangeProtocolVaultStorage.sol	Acknowledged

Description

The contract is serving as the underlying entity to interact with one or more third party protocols. The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of third parties can possibly create severe impacts, such as increasing fees of third parties, migrating to new LP pools, etc.

```
23      address public immutable factory;
```

- The contract `RangeProtocolFactory` interacts with third party contract with `IUniswapV3Factory` interface via `factory`.

```
18      IUniswapV3Pool public pool;
19      IERC20Upgradeable public token0;
20      IERC20Upgradeable public token1;
```

- The contract `RangeProtocolVaultStorage` interacts with third party contracts with `IUniswapV3Pool` and `IERC20Upgradeable` interfaces via `pool`, `token0` and `token1`.

```
78          pool = IUniswapV3Pool(_pool);
79          token0 = IERC20Upgradeable(pool.token0());
80          token1 = IERC20Upgradeable(pool.token1());
```

- The contract `RangeProtocolVault` interacts with third party contracts with `IUniswapV3Pool` and `IERC20Upgradeable` interfaces via `pool`, `token0` and `token1`.

Recommendation

We understand that the business logic requires interaction with the third parties. We encourage the team to constantly monitor the statuses of third parties to mitigate the side effects when unexpected activities are observed.

Alleviation

[Range Team]:

We will actively monitor the dependency contracts and change the vault configuration to adapt to any changes (if required).

RPB-03 | INCOMPATIBILITY WITH DEFLATIONARY TOKENS

Category	Severity	Location	Status
Logical Issue	Minor	contracts/RangeProtocolFactory.sol; contracts/RangeProtocolVault.sol; contracts/RangeProtocolVaultStorage.sol	Acknowledged

Description

When transferring deflationary ERC20 tokens, the input amount may not be equal to the received amount due to the charged transaction fee. For example, if a user sends 100 deflationary tokens (with a 10% transaction fee), only 90 tokens actually arrived to the contract. However, a failure to discount such fees may allow the same user to withdraw 100 tokens from the contract, which causes the contract to lose 10 tokens in such a transaction.

Recommendation

We advise the client to regulate the set of tokens supported and add necessary mitigation mechanisms to keep track of accurate balances if there is a need to support deflationary tokens.

Alleviation

[Range Team]:

We have no plans to support vaults for deflationary tokens at this point.

RPV-03 | DISCUSSION ON OWNERABLE CONTRACT

Category	Severity	Location	Status
Logical Issue	Minor	contracts/RangeProtocolVault.sol: 35~43	Resolved

Description

We noticed that the current Ownerable contract is a forked and modified version of OpenZeppelin's contract. If the main purpose of using it is to set a `_manager` different from `msg.sender`, it can be done by deploying the contracts and then calling `transferOwnership()` function. Also, upgradeable contract must extend upgradeable contracts and call initializer functions of parent-contracts in its own initializer function. Otherwise, it may malfunction due to improper initialization or improper upgrading.

Recommendation

Recommend using `OwnableUpgradeable` in the contract `RangeProtocolVault`.

Alleviation

[Range Team]:

We have modified the factory contract to use non-upgreadble Ownable contract from Openzeppelin and Vault contract is modified to use a modified version of Ownable contract that is based on upgradeable version of ownable contract from Openzeppelin. The changes have been performed in the commit hash https://github.com/Range-Protocol/contracts/tree/4d822ceabdd6b4be712c8d2610be3b3ae673522d

RPV-04 | LACK OF RETURN VALUE HANDLING

Category	Severity	Location	Status
Volatile Code	Minor	contracts/RangeProtocolVault.sol: 202, 609	Acknowledged

Description

The return values of external calls are not stored in a local or state variable.

```
202             pool.mint(address(this), lowerTick, upperTick, liquidityMinted,
"");
```

```
609         pool.collect(address(this), _lowerTick, _upperTick, type(uint128).max,
type(uint128).max);
```

Recommendation

We recommend checking or using the return values of all external function calls.

Alleviation

[Range Team]:

We are not intentionally using the returned values since we are not using them and in case "mint" or "collect" call fails for any reason the transaction reverts.

GLOBAL-02 DISCUSSION ON THE VAULT MANAGER RESPONSIBILITIES

Category	Severity	Location	Status
Business Model	Informational		Acknowledged

Description

Our current understanding is that for external users, their investment for Range Protocol highly relies on the vault manager to update the ticks, swap tokens, and add/remove liquidity to/from the vault. Impermanent loss or opportunity cost would take place if the price of the token pair moves outside of the chosen price range. This means that the liquidity providers would lose their exposure to one of the tokens and stop earning fees until the price reenters the range. This could result in lower returns or losses compared to holding the tokens outside of Uniswap or providing liquidity across the entire price curve. Moreover, if the price moves significantly or rapidly outside of the range, it might be costly or difficult for the vault manager to update the ticks or swap tokens to adjust to the new market conditions. If the price moves significantly or rapidly outside of the range, it might be costly or difficult for the vault manager to update the ticks or swap tokens to adjust to the new market conditions.

Please feel free to correct our speculations if there are any misunderstanding, and here are what to confirm:

1. We would like to confirm the responsibility of the vault manager? Will it be an off-chain script or program that will manage the on-chain contracts automatically? Or will it be a human sit behind the vault manager address?

2. We would like to confirm if there are plans to open the access of creating vaults to all users or maybe selected users in the future? If so, how to make sure that the vault mangers not doing harm?

Recommendation

N/A

Alleviation

[Range Team]:

1. The manager of the vault will be responsible for managing LP's liquidity and provide best possible yield. The managers will be sophisticated trading tasks running algorithmic strategies that will be actively managing the liquidity.
2. We will only enable sophisticated trading partners to deploy vaults. There are no plans currently permissionless and enable anyone to deploy vaults. We will partner up with market makers and trading partners and then deploy vaults for them to manage.

GLOBAL-04 | DISCUSSION ON USER STRATEGY

Category	Severity	Location	Status
Business Model	Informational		Acknowledged

Description

We noticed that users can freely call `mint()` and `burn()` functions as long as they have enough `token0` / `token1` to trade for the vault token or vice versa. The users cannot choose how to maximize their output by deciding when to mint/burn, or deciding how long they would like to hold the Range token, etc. We would like to learn that are there any trading/staking strategies that are pre-considered during the project design phase?

Recommendation

N/A

Alleviation

[Range Team]:

This is the underlying behavior with providing liquidity to Uniswap v3 pool as the composition of LP token keeps changing as price moves. We will make the current vault composition visible on the frontend and the managers of the vault will structure their strategies in a way to maintain beta exposure so that users can quantify their returns compared to holding their initial portfolio in spot. Future iterations will have the option for users to swap through the frontend to enter even if they dont have tokens in the exact ratio of the vault but it would have an associated slippage.

RPV-06 | WRONG FEE VALUE EMITTED

Category	Severity	Location	Status
Data Flow	Informational	contracts/RangeProtocolVault.sol: 228~231, 285~288, 392~395	Acknowledged

Description

The event `PerformanceFeeEarned()` is usually emitted after function calls of `_applyPerformanceFee()` and `_netPerformanceFees()`, where `_applyPerformanceFee()` calculates the fees and adds to the manager balance, and `_netPerformanceFees` returns the value after fee decuction.

However, unlike event `ManagingFeeEarned()`, the values to be emitted are like `amount0 - amount0AfterFee` and `amount1 - amount1AfterFee`. The values emitted by `PerformanceFeeEarned()` are `fee0` and `fee1`, which are value after fee deduction, instead of the fee earned.

Recommendation

Recommend reviewing the use cases and update the values to be emitted or the event name.

Alleviation

In the commit hash 4d822ceabdd6b4be712c8d2610be3b3ae673522d, `ManagingFeeEarned` is removed, and `PerformanceFeeEarned` is renamed to be `FeesEarned`

[Range Team]:

Issue acknowledged. The changes has been performed in the following commit https://github.com/Range-Protocol/contracts/tree/4d822ceabdd6b4be712c8d2610be3b3ae673522d

OPTIMIZATIONS | RANGE PROTOCOL

ID	Title	Category	Severity	Status
RPV-05	Unnecessary Checks For `uint` Type Variables	Gas Optimization	Optimization	Resolved

RPV-05 | UNNECESSARY CHECKS FOR `uint` TYPE VARIABLES

Category	Severity	Location	Status
Gas Optimization	Optimization	contracts/RangeProtocolVault.sol: 422, 426	Resolved

Description

Comparisons that are always true or always false may be incorrect or unnecessary.

```
422         if (newManagingFee >= 0) {
```

```
426         if (newPerformanceFee >= 0) {
```

Recommendation

Recommend reviewing the design and fixing the if statements to be meaningful.

Alleviation

[Range Team]:

Issue acknowledged. The changes have been performed in the following commit. https://github.com/Range-Protocol/contracts/tree/4d822ceabdd6b4be712c8d2610be3b3ae673522d

APPENDIX | RANGE PROTOCOL

Finding IDs

Each finding will have a unique finding ID. Finding IDs will be consistent in preliminary comments and security assessments. They are not necessarily consecutive. This means in published report there will be skipped finding ID numbers, which is intentional.

Finding Categories

Categories	Description
Gas Optimization	Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.
Logical Issue	Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.
Control Flow	Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.
Data Flow	Data Flow findings describe faults in the way data is handled at rest and in memory, such as the result of a struct assignment operation affecting an in-memory struct rather than an in-storage one.

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.