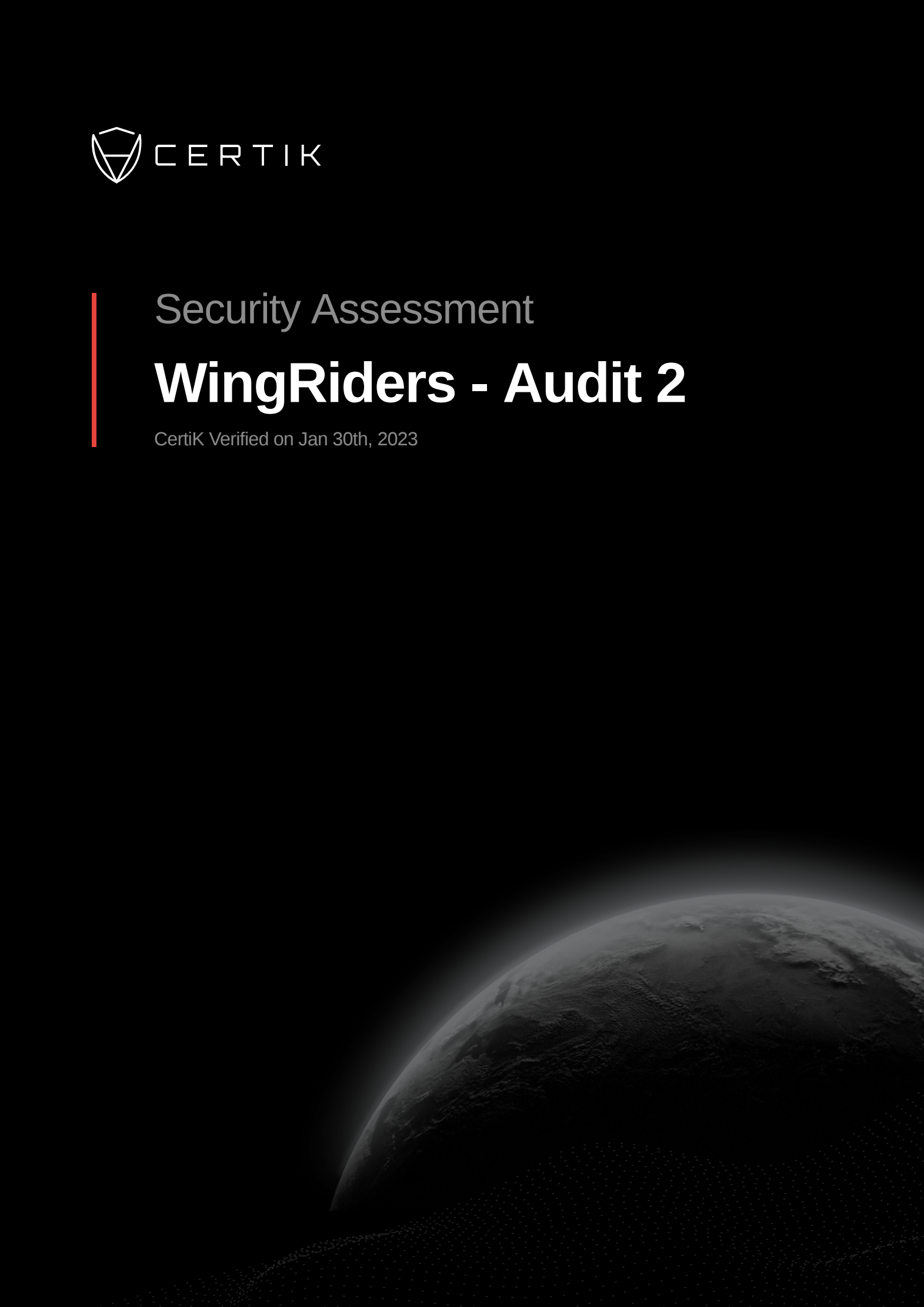
CERTIK

Security Assessment

# WingRiders - Audit 2

CertiK Verified on Jan 30th, 2023




CertiK Verified on Jan 30th, 2023

# WingRiders - Audit 2

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

## Executive Summary

| TYPES | ECOSYSTEM | METHODS |
|---|---|---|
| DeFi | Cardano | Manual Review |

| LANGUAGE | TIMELINE | KEY COMPONENTS |
|---|---|---|
| haskell | Delivered on 01/30/2023 | N/A |

CODEBASE

https://github.com/WingRiders/

...View All

COMMITS

0c5ca5c437d3fb9eff44c12813119c3074417f1b

579aed64ac659b7f43772e1785ab4ea6d619dcaa

...View All

## Vulnerability Summary

| 3 | 3 | 0 | 0 | 0 | 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. |
| 0 | Medium | | Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform. |
| 0 | Minor | | Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions. |
| 3 | Informational | 3 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 | WINGRIDERS - AUDIT 2

# CODEBASE | WINGRIDERS - AUDIT 2

## Repository

https://github.com/WingRiders/

## Commit

0c5ca5c437d3fb9eff44c12813119c3074417f1b
579aed64ac659b7f43772e1785ab4ea6d619dcaa

# AUDIT SCOPE | WINGRIDERS - AUDIT 2

5 files audited ● 2 files with Resolved findings ● 3 files without findings

| ID | File | SHA256 Checksum |
|---|---|---|
| ● SAM | src/DEX/OnChain/Core/StableswapAMM.hs | 60c149b7f9e0fbfba8cf9b41483d037606792b3d975d23dc5e0c43e039d8e3e2 |
| ● SPC | src/DEX/OnChain/Core/StableswapPool.hs | 4334a163d4bb9abe5323576c3dbf5e51ddd86f1273bb040229f7def81b506a63 |
| ● SPS | src/DEX/OnChain/Core/StableswapPoolState.hs | f14b47d6320bf70e8e9d75643a9fb8785861ce57696aa0d2bb82dd19590a9550 |
| ● SFO | src/DEX/OnChain/StableswapFactory.hs | 424fac158fed4de8b35b0ee40ba4f4c59e57e8d78d6507869f29fd2541e2e1ab |
| ● SPO | src/DEX/OnChain/StableswapPool.hs | 57100366d0ae5f0a6f464f8604f2b3ac6e6251fc82355ad592b064a9eb647106 |

# APPROACH & METHODS | WINGRIDERS - AUDIT 2

This report has been prepared for WingRiders to discover issues and vulnerabilities in the source code of the WingRiders - Audit 2 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.

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 at the informational level only. We recommend addressing these findings to ensure a high level of security standards and industry practices.

# REVIEW NOTES | WINGRIDERS - AUDIT 2

WingRiders is a decentralized exchange (DEX) on the Cardano blockchain, which provides a constant-function automatic market maker. The WingRiders operator creates trading pools containing reserves of two different tokens, and users can either provide liquidity to the pool by depositing tokens into it, or use it to trade one token for another. In order to perform well on the Cardano eUTxO model, WingRiders adopts a batched approach, where orders are submitted via a batching agent who will gather them into batches of multiple orders.

CertiK previously audited the entire WingRiders on-chain contracts (as described in a previous report). At that point it implemented the UniSwap-style constant product equation, i.e. the amount of reserves $x$ and $y$ satisfies $xy = k$ for some $k$. Now it adds support for pools using the StableSwap equation, and in this report we describe our new audit of the added code.

The StableSwap equation is

$$4xy(4A(x+y)+D) = 16ADxy + D^3.$$

Here $A$ is a fixed constant affecting the shape of the curve (in WingRiders $A = 75$) and $D$ is a measure of how much reserves have been deposited in the contract (analogous to $k$ in the constant product formula). This equation is now commonly used by various automatic market makers. Compared to the constant-product formula, it is closer to linear in the region where $x \approx y$. This makes it suitable for pairs of tokens where the price is expected to not fluctuate much, because then it can execute larger trades with small price slips, so it makes more efficient use of the deposited liquidity.

The main operations which we audit are (1) creating new pool, initialized to suitable values. (2) Supplying or withdrawing liquidity from the pool. (3) Executing a trade.

WingRiders is implemented in the Plutus programming language. There are some aspects that depend on the characteristics of Cardano and Plutus:

- Because it is implemented using integer arithmetic rather than real numbers, the equation is not satisfied exactly. Therefore, the contracts check that $D$ satisfies it to the nearest integer, rounded in the right direction (so that the pool does not lose money from rounding).
- For efficiency the general style is to validate rather than compute: the user provides the desired trading amounts, and the contract checks that they will satisfy the equation.
- The trade also incurs a trading fee. Conceptually this is put into a "treasury", to be withdrawn by the pool operator later. However, both reserves and treasury are stored as Plutus values on the same UTxO, so the contract maintains a record in the UTxO datum of how much reserves and treasury it has, and the actual value should be equal to the sum of these.

In the audit, we particularly studied that the mathematical formula was implemented correctly, and also that this business logic was integrated suitably into the existing contract code for executing requests.

# FINDINGS | WINGRIDERS - AUDIT 2

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

This report has been prepared to discover issues and vulnerabilities for WingRiders - Audit 2. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Manual Review to complement rigorous manual code reviews, we discovered the following findings:

| ID | Title | Category | Severity | Status |
|---|---|---|---|---|
| SAM-01 | Use Existing Constant | Magic Numbers | Informational | Resolved |
| SAM-02 | Inconsistent Comments | Inconsistency | Informational | Resolved |
| SPC-01 | Typos | Coding Style | Informational | Resolved |

# SAM-01 | USE EXISTING CONSTANT

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Magic Numbers | Informational | src/DEX/OnChain/Core/StableswapAMM.hs (0c5ca5c437d3fb9eff44c12813119c3074417f1b): 30 | Resolved |

## Description

The literal `10000` is used instead of `swapFeeBasis` defined with the same value in `DEX.OnChain.Common.StableswapProtocolParams`.

## Recommendation

Use the defined value `swapFeeBasis` in `DEX.OnChain.Common.StableswapProtocolParams` instead of the literal `10000`.

## Alleviation

`[CertiK]`: The team heeded the advice and resolved the finding in the commit hash 579aed64ac659b7f43772e1785ab4ea6d619dcaa.

# SAM-02 | INCONSISTENT COMMENTS

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Inconsistency | Informational | src/DEX/OnChain/Core/StableswapAMM.hs (0c5ca5c437d3fb9eff44c12813119c3074417f1b): 34~35 | Resolved |

## Description

In `StableswapAMM.hs` the comment before the function `stableswapProtocolFee` states that the amount of fees for the treasury is 0.01% of the `locked amount` which represents 1/6 of the swap fee, meaning that the amount of fee returned to the pool is 0.05%.
This contradicts the following comments of the function `swapFeeInBasis` from the file `StableswapProtocolParams.hs`:

```
24  --  0.06% is returned in the pool for liquidity providers.
25  --  0.01% goes into the treasury
```

## Recommendation

We recommend correcting the comments.

## Alleviation

`[CertiK]`: The team heeded the advice and resolved the finding in the commit hash 32e100b2cb16b9bdb1af1d3c9785915b5fb281c8.

# SPC-01 | TYPOS

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Coding Style | Informational | src/DEX/OnChain/Core/StableswapPool.hs (0c5ca5c437d3fb9eff44c12813119c3074417f1b): 165, 326 | Resolved |

## Description

The contract contains typos that need to be changed as follows:

```
165        -- The pool and agnet are distinct utxos enforced by the `agentChecked`.
```

should be written:

```
      -- The pool and agent are distinct utxos enforced by the `agentChecked`.
```

```
326  --  This function throws is request is not applied correctly.
```

should be written

```
326  --  This function throws if the request is not applied correctly.
```

## Recommendation

We recommend correcting the typos to improve readability.

## Alleviation

`[CertiK]`: The team heeded the advice and resolved the finding in the commit hash 206fc112dc96efcc1cea7e0213476676a04e31fc.

# APPENDIX | WINGRIDERS - AUDIT 2

## Finding Categories

| Categories | Description |
| --- | --- |
| Coding Style | Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable. |
| Inconsistency | Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different require statements on the input variables than a setter function. |
| Magic Numbers | Magic Number findings refer to numeric literals that are expressed in the codebase in their raw format and should otherwise be specified as constant contract variables aiding in their legibility and maintainability. |

## 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.