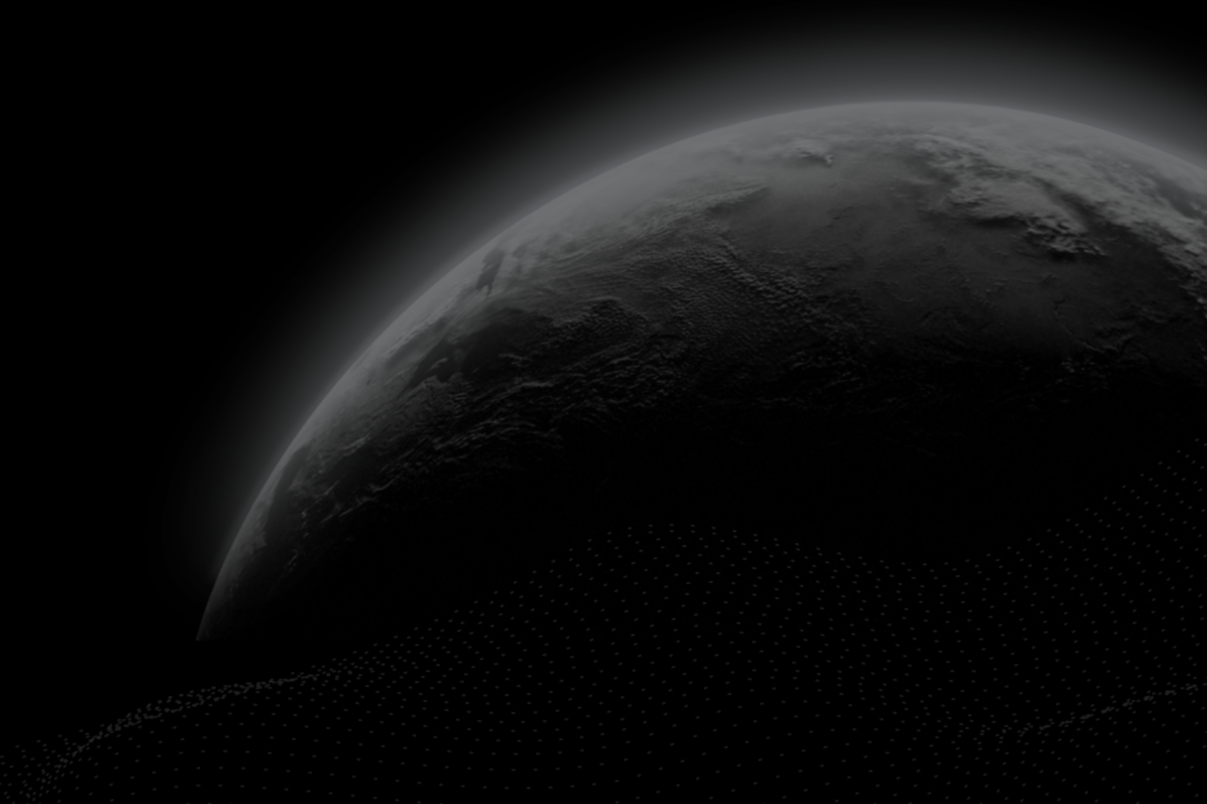
CERTIK

Security Assessment

Folks Finance - Audit 1

CertiK Verified on Dec 12th, 2022



CertiK Verified on Dec 12th, 2022

Folks Finance - Audit 1

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Algorand (ALGO)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
pyteal	Delivered on 12/12/2022	N/A

CODEBASE	COMMITS
https://github.com/blockchain-italia/ff-certik-contracts/tree/93b558080137fcf578acc9469cc4df682612baed/contracts/f_staking ...View All	93b558080137fcf578acc9469cc4df682612baed ...View All

Vulnerability Summary

3	0	1	0	2	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.
🟧	1	Major	1 Mitigated	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.
🟨	1	Minor	1 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.
🟦	1	Informational	1 Acknowledged	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | FOLKS FINANCE - AUDIT 1

CODEBASE | FOLKS FINANCE - AUDIT 1

Repository

https://github.com/blockchain-italia/ff-certik-contracts/tree/93b558080137fcf578acc9469cc4df682612baed/contracts/f_staking

Commit

93b558080137fcf578acc9469cc4df682612baed

AUDIT SCOPE | FOLKS FINANCE - AUDIT 1

9 files audited ● 1 file with Acknowledged findings ○ 8 files without findings

ID	File	SHA256 Checksum
● FCK	projects/FolksFinance/contracts/f_staking/f_staking.py	d6ab0350d508b544f02692d2748d1248828828a760cf8cdd68c7bd0fd508fe0e
○ FFK	projects/FolksFinance/contracts/f_staking/__init__.py	
○ FFP	projects/FolksFinance/contracts/f_staking/f_staking.json	e9d3696c85c18ff058864200740edcbe32b108bd1404cd5f10f6af89854a079f
○ FCP	projects/FolksFinance/contracts/f_staking/f_staking_state.py	bd4e19b5c904a1fa2c44833519e14b79d3cfae81e316f6c84cdb5dbcdb612ba1
○ CKP	projects/FolksFinance/contracts/common/helpers/__init__.py	
○ ARR	projects/FolksFinance/contracts/common/helpers/array.py	0b037ee09d7de3aa953e7fdac675a27924b7d7d47ed9ee803054326c919d206a
○ INN	projects/FolksFinance/contracts/common/inner_txn.py	c3b9e2f272c6827999b50f0d520f9beb40449b28605952a44bcad5e4d9c1bd4b
○ CHE	projects/FolksFinance/contracts/common/checks.py	3772aae23900ffec0d8229e2b06db2c974d571f6bc7fe6dd7bb023c5c0ba497e
○ MAT	projects/FolksFinance/contracts/common/math_lib.py	b2747abbedd34dc0457f3866b280fc1eea1b737a5eb1987b73dafa30b4a4e141

APPROACH & METHODS | FOLKS FINANCE - AUDIT 1

This report has been prepared for Folks Finance - Audit 1 to discover issues and vulnerabilities in the source code of the Folks Finance - Audit 1 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.

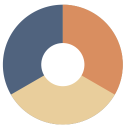
The auditing process pays special attention to the following considerations:

- 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.

FINDINGS | FOLKS FINANCE - AUDIT 1



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

This report has been prepared to discover issues and vulnerabilities for Folks Finance - Audit 1. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
FCK-01	**Centralization Related Risks**	**Centralization / Privilege**	**Major**	● **Mitigated**
FCK-02	Potential Loss Of Precision	Mathematical Operations	Minor	● Acknowledged
GLOBAL-01	Out Of Scope Dependencies	Volatile Code	Informational	● Acknowledged

FCK-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization / Privilege	● **Major**	**projects/FolksFinance/contracts/f_staking/f_staking.py: 251 , 265, 292, 354, 378, 410**	● **Mitigated**

Description

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

- function update_admin()
- function add_staking_program()
- function add_reward_asset()
- function update_end()
- function update_reward_rate()
- function withdraw_rewards()

Any compromise to the admin account may allow a hacker to take advantage of this authority and cause the malfunction of the protocol.

In addition, there is no guarantee that there is enough reward balance in the application. The admin can withdraw rewards at any time for any amount by calling function `withdraw_rewards` , and users might not get rewards for the time they already staked.

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 recommend carefully managing 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., multi-signature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of long-term and permanent:

Long Term:

- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND

- Introduction of a DAO/governance/voting module to increase transparency and user involvement;
  AND
- A medium/blog link for sharing the 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

[Folks Finance Team]:

We use a multisig account Q5Q5FC5PTYQIUX5PGNTEW22UJHJHVVUEMMWV2LSG6MGT33YQ54ST7FEIGA.

Building a DAO is on our upcoming roadmap.

FCK-02 | POTENTIAL LOSS OF PRECISION

Category	Severity	Location	Status
Mathematical Operations	● Minor	projects/FolksFinance/contracts/f_staking/f_staking.py: 54~58, 79	● Acknowledged

Description

In the function `update_reward_per_token` , the timestamp is converted to uint32 in line 79 and stored to the reward array, which will cause precision loss during the conversion. The stored timestamp is used to compared with `Global.latest_timestamp()` . If the precision loss is substantial, the result of the comparison might be affected.

Recommendation

We recommend the team elaborate the reason behind the conversion.

Alleviation

[Folks Finance Team]: The reason why we use uint32 is because it saves on limited storage space in global state. A uint32 supports unix time till year 2106 so there is no concern with using it.

GLOBAL-01 | OUT OF SCOPE DEPENDENCIES

Category	Severity	Location	Status
Volatile Code	● Informational		● Acknowledged

Description

The scope of the audit treats out-of-scope Folks finance pool contracts as black boxes and assumes their functional correctness. However, in the real world, those contracts can be compromised and this may lead to lost or stolen assets. Additionally, upgrades of those contracts can possibly create severe impacts.

Recommendation

The aforementioned contracts are out of the audit scope. We encourage the team to constantly monitor the statuses of those contracts to mitigate the side effects when unexpected activities are observed.

Alleviation

[Folks Finance Team]:

These smart contracts have / are being audited by two other firms.

APPENDIX | FOLKS FINANCE - AUDIT 1

Finding Categories

Categories	Description
Centralization / Privilege	Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.
Mathematical Operations	Mathematical Operation findings relate to mishandling of math formulas, such as overflows, incorrect operations etc.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

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.