SMART CONTRACT AUDIT PUBLIC REPORT

Revision Audit of Liquid Governance v3

VPQ-2022046

BlockchainItalia.io - Folks Finance

28th September 2022

VANTAGEPOINT

Security at the Speed of Development

CREST

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

OVERVIEW

Vantage Point Security Pte Ltd was engaged by Folks Finance to conduct an Algorand smart contract revision audit on the changes made to the Folks Finance Liquid Governance contract as part of its changes, in line with Algorand Governance 5.

The new Folks Finance Liquid Governance v3 (FFLGv3) smart contract includes changes to both existing operations and new operations, such as unmint_premint and on_claim_premint, to prevent users from abusing the overlap in duration of the following operations:

1. Burning of gAlgo from Folks Finance Liquid Governance v2 (FFLGv2) smart contract (Distributor App ID – 793119270)
2. Minting of gAlgo from FFLGv3 smart contract

When burning operations with FFLGv2 and minting operations with FFLGv3 are allowed simultaneously, any user can mint gAlgo from FFLGv3 and be eligible for Governance 5 rewards pool without committing Algo. This is because the gAlgo can be burned through the FFLGv2 once the Governance 4 period ends. To avoid such abuse, premint feature is introduced as a preventative measure by setting the premint_end value to when FFLGv2 has stopped allowing burning operations. Before the premint_end period, all mint operations will be treated as "premint" operations as only local and global states are updated and no gAlgo is given until the on_claim_premint operation is called after the premint_end period.

Smart contract revision audit was conducted based on the following materials provided.

- Supporting Documents
  - Documentation - Algo Liquid Governance v3
- PyTeal Code
  - https://github.com/blockchain-italia/ff-vp-contracts 5d9ec188e6e24c6b22ddd470b6bf815a82f33d73

Vantage Point performed this review by first understanding the changes to the Folks Finance liquid governance protocol in support of new operations related to Premint functionality including changes to existing operations. We sought clarifications on potential issues, discrepancies, flaws, and plans on how manual operations involved would be carried out through discussions with the Folks Finance team.

A revision audit was conducted on the provided PyTeal code to identify any weaknesses, vulnerabilities, and non-compliance to Algorand best practices from the introduced changes to the code. Test cases included in this review have been amended in the appendix of this document for reference.

The following informational issue was was noted from this revision audit.

1. **Inaccurate Comments**
   Based on the provided PyTeal code in scope, the smart contract's code comments contained incorrect description of the expected transaction details, especially its transaction arrays which are often used to supply required parameters for the operations such as Txn.accounts, Txn.assets, Txn.applications and Txn.application_args. Having incorrect comments may create unnecessary confusion in providing context to future development efforts in making changes to or integrating with the reviewed smart contract.

The outcome of this Algorand Smart Contract Revision Audit engagement is provided as a detailed technical report that provides the project owners a full description of the vulnerabilities identified, the associated risk rating for each vulnerability, and detailed recommendation that will resolve the identified technical issue.

VULNERABILITY OVERVIEW

Severity	Count	Open	Closed
Critical	**0**	**0**	**0**
High	**0**	**0**	**0**
Medium	**0**	**0**	**0**
Low	**0**	**0**	**0**
Observational	**1**	**0**	**1**
Summary	**1**	**0**	**1**

Vulnerability Risk Score

All vulnerabilities found by Vantage Point will receive and individual risk rating based on the following four categories.

CRITICAL COMPONENT RISK SCORE

Critical severity findings relate to an issue, which requires immediate attention and should be given the highest priority by the business as it will critically impact business interest critically.

HIGH COMPONENT RISK SCORE

HIGH severity findings relate to an issue, which requires immediate attention and should be given the highest priority by the business.

MEDIUM COMPONENT RISK SCORE

A MEDIUM severity finding relates to an issue, which has the potential to present a serious risk to the business.

LOW COMPONENT RISK SCORE

LOW severity findings contradict security best practice and have minimal impact on the project or business.

OBSERVATIONAL

Observational findings relate primarily to non-compliance issues, security best practices or are considered an additional security feature that would increase the security stance of the environment which could be considered in the future versions of smart contract.

2. PROJECT DETAILS

SCOPE

Contact Name	Gidon Katten
Application Name	Folks Finance Liquid Governance V3
SVN / GIT Revision Number	5d9ec188e6e24c6b22ddd470b6bf815a82f33d73
Items Completed	assets/algo_governance/state.py assets/algo_governance_distributor_approval_program.py

Component	Review Type	Status
Algorand Smart Contract	Smart Contract Security Revision Audit	Completed
Algorand Smart Contract	Smart Contract Security Revision Audit Retest	Completed

VERSION HISTORY

Date	Version	Release Name
26th September 2022	V0.1	Draft
28th September 2022	V0.2	QA Release
28th September 2022	V1.0	Final
28th September 2022	V1.1	Code Snippet Removal

3. Risk Assessment

This chapter contains an overview of the vulnerabilities discovered during the project. The vulnerabilities are sorted based on the risk categories of CRITICAL, HIGH, MEDIUM, and LOW. The category OBSERVATIONAL refers to vulnerabilities that have no risk score and therefore have no immediate impact on the system.

Overview of Components and Their Vulnerabilities

1. Revision Audit of Liquid Governance		OBSERVATIONAL
1.1. Inaccurate Comments	Closed	OBSERVATIONAL

4. Detailed Description of Vulnerabilities

2. Revision Audit of Liquid Governance — OBSERVATIONAL

1.1. Inaccurate Comments

OBSERVATIONAL

VULNERABILITY TRACKING

STATUS: **Closed**

BACKGROUND

Code comments play a vital role in providing context to the readers of the code so that technical specifications, transactions details, and requirements can be clearly conveyed to users or future development team members. Inaccurate comments could cause confusion to users and developers who may rely on the information provided in understanding the logic of the smart contract.

DESCRIPTION

Affected File/Code:

- https://github.com/blockchain-italia/ff-vp-contracts/blob/master/assets/algo_governance_distributor_approval_program.py
  - on_claim_premint() - Line 307

It was noted that the smart contract code had incorrect comments for the above operation/method.

Following issues were noted.

- Txn.application_args() is missing the index for Txn.assets() array
- Txn.assets() is missing ASA ID of the asset being received
- Txn.accounts is missing receiver's account address

- InnerTransaction is expected to be an application call to dispenser smart contract which triggers another AssetTransferTx

RECOMMENDATION

Update comments according to the latest business logic and technical specifications to ensure the understanding of the readers are coherent.

REGRESSION TESTING COMMENT

26th September 2022 - This issue is closed.

As the commit 66babdda05374d635e0cc3246ee240bb138748de contains changes to below part of the code which updates the inaccurate comments within the smart contract, this issue is closed.

- **assets/algo_governance_distributor_approval_program.py - Line 297-314**

VULNERABILITY REFERENCES

CWE-1116: Inaccurate Comments

https://cwe.mitre.org/data/definitions/1116.html

5. APPENDIX

DISCLAIMER

The material contained in this document is confidential and only for use by the company receiving this information from Vantage Point Security Pte. Ltd. (Vantage Point). The material will be held in the strictest confidence by the recipients and will not be used, in whole or in part, for any purpose other than the purpose for which it is provided without prior written consent by Vantage Point. The recipient assumes responsibility for further distribution of this document. In no event shall Vantage Point be liable to anyone for direct, special, incidental, collateral or consequential damages arising out of the use of this material, to the maximum extent permitted under law.

The security testing team made every effort to cover the systems in the test scope as effectively and completely as possible given the time budget available. There is however no guarantee that all existing vulnerabilities have been discovered due to the nature of manual code review. Furthermore, the security assessment applies to a snapshot of the current state at the examination time.

SCOPE OF AUDIT

Vantage Point reviewed the smart contracts underlying codebase to identify any security or economic flaws, or non-compliance to Algorand best practices. The scope of this review included the following test-cases and audit points.

- Insufficient Sender Address Validation for Privileged Operations
- Lack of Validation for Validity of Referenced States from External Applications
- Insufficient Validation of Transaction Fields and Types
- Validation of RekeyTo address for non-rekeying transactions
- Validation of CloseRemainderTo and AssetCloseTo for non-closing transactions
- Validation of Asset Identifier for Asset Transfer Transactions
- Validation of GroupIndex and GroupSize for Transaction Groups
- Incorrect Order of Operations
- Smart Contract Versions
- Incorrect Use of ScratchVar, Local and Global States
- Flawed/Inaccurate Logical/Mathematical Operations
- Overflow or Underflow Possibilities based on Valid Argument Ranges
- Validation of user-supplied Application Arguments
- Use of Multisignatures for Privileged Accounts
- Other known Algorand Best Practices and Guidelines