Smart Contract Audit

Algofi Algo Vault

coinspect

Algofi Algo Vault

Smart Contract Audit

V220329

Prepared for Algofi • March 2022

1. Executive Summary

In **March 2022, Algofi** engaged Coinspect to perform a source code review of the new **Algo Vault** being added to the Algofi Protocol. The objective of the project was to evaluate the security of the smart contracts.

The audit focused on the changes performed to the protocol since a previous audit performed by a third party, assuming the audited code is considered secure. Specifically, Coinspect efforts concentrated on PR#287 which implements the new Algo Vault feature. Per the client's request, Coinspect focused on the Algo Vault and governance logic within the scope of the lending protocol. Other components were only reviewed when required in order to understand how the new code interacts with the rest of the system, as the new Algo Vaults implement a reduced subset of Algofi's Markets functionality.

Coinspect did not identify any security vulnerabilities in the code introduced by Algofi after the previous security audit performed by a third party. The new features were implemented following Algorand security best practices and did not break any security assumptions in the existing code.

No security issues were identified during the assessment:

High Risk	Medium Risk	Low Risk
0	0	0
Fixed -	Fixed -	Fixed -

2. Assessment and Scope

The audit started on **March 21, 2022** and was conducted on the **feature/algo-vault** branch of the git repository at https://github.com/Algofiorg/algofi-protocol as of commit **efcb7a2a73bbbf9707d80b2aae23da4edabf7ed6** of **March 17, 2022**:

```
9a182b75e10df140048237cb3c0f56d9dd66893261e59c18caea27d294809998  manager.py
1bc94ba29ad997c018fbe9f4aa5169f1f30b123bdd21f07fd5c929475ddcbe78  algo_vault_market.py
7d7485422ce2d4e9379e95694c184a861cb62582d8f8d63038aebf2c87f22473  market.py
35073edd1b92443d1bda515eb86f4424c94193ee4c064eb44dfdf1e743f28b8f  wrapped_var.py
1838420721ae7363bf1eb531191f83c295bfa522e69d433ba089af573d57ed22  oracle.py
ccce4e48c036823622ec3407f1fde38e9dfcb69761162f159a0e55256c32516d  globals.py
62ade17457ba3b30b4ab2b8f6651b0328bc53688ad376e9601ebc8c7a4871c7e  opt_out_manager.py
```

The Algofi protocol provides users with a decentralized lending and borrowing market, plus a stablecoin on the Algorand blockchain. The new Algo Vaults implement a liquid staking mechanism. They are intended to allow users to continue to earn rewards from staking their Algos and participating in Algorand's governance and consensus, while being able to utilize the derived vault tokens to obtain yield in other DeFi protocols at the same time.

Coinspect audited the changes introduced on the platform in order to support the Algo Vaults feature. The new code was examined, looking for common Algorand smart contracts implementation pitfalls and any potential issues that could break the security assumptions and invariants present in the existing code. No security issues were identified during this engagement.

The most important changes were performed to the existing `manager.py` contract, and the addition of the `new algo_vault_market`.

The new `algo_vault_market.py` contract consists in a simplified version of the already existing `market.py` one: several application calls were removed as they are no longer supported as a result of the funds in this vault being locked. The new `sync_vault` function was added in order to allow users to synchronize the funds earned and sent directly to their vault with the current protocol state. Algo vaults only support Algos as collateral, no other assets can be used with this market.

Coinspect recommends removing the code no longer being used in the contract, e.g. the code responsible for interest rate calculations that no longer make sense in the Algo vaults.

In the Algorand blockchain, users can forcefully delete their storage in a contract, including their debts. To prevent this issue while allowing the user to still control their funds, the Algofi team created the storage account: an account rekeyed to the manager that can be operated by the original user in a limited way. The `manager.py` contract incorporates two important new functions that allow users to participate in governance by casting votes. Also, there is a new function that allows retrieving the vaulted Algos. Only the Vault Market can request the Manager that the vaulted Algos be retrieved from their corresponding storage account.

Coinspect observed the TEAL version used to compile the applications in the protocol was upgraded from 5 to 6 in a change performed in the `onchain_utils.py` file.

3. Disclaimer

The information presented in this document is provided "as is" and without warranty. The present security audit does not cover any off-chain systems or frontends that communicate with the contracts, nor the general operational security of the organization that developed the code.