SOLIDIFIED

Audit Report for Pods on July 28th, 2020.

Summary

Audit Report prepared by Solidified for Pods covering their options platform smart contracts (and associated components).

Process and Delivery

Three (3) independent Solidified experts performed an unbiased and isolated audit of the code below. The debrief took place on July 28th, 2020, and the final results are presented here.

Audited Files

The following contracts were covered during the audit:

```
https://github.com/pods-finance/contracts
```

- aOptionFactory.sol
- aPodPut.sol
- OptionsExchange.sol
- OptionFactory.sol
- PodOption.sol
- PodPut.sol
- waPodPut.sol
- wPodPut.sol
- ExchangeProvider.sol
- BalancerProvider.sol
- UniswapV1Provider.sol

Notes

The audit was based on commit `a94e860327e936191d1e5a363d7e20c4a3999354`, Solidity compiler version `0.6.8`.

Intended Behavior

The Pods contracts implement American type options between any two ERC20 assets or ETH, using physical settlement in order to negate the need for an oracle.

SOLIDIFIED

Audit Report for Pods on July 28th, 2020.

Executive Summary

Solidified found that the Pods contracts four minor issues, in addition to several areas of note. We recommend all issues are amended before deployment, with notes being up to Pods' discretion, since they pose no security risk and refer mainly to best practices.

Follow up [22.09.2020]
All issues were fixed and are no longer present in commit `2b0f9a5217a6901d17c1e907fe1f0107dd2e86ff`.

Issues Summary

Critical	Major	Minor	Notes
0	0	4	6

SOLIDIFIED

Audit Report for Pods on July 28th, 2020.

Issues Found

Critical Issues

No critical issues were found.

Major Issues

No major issues were found.

Minor Issues

1. A non existing Uniswap market will break the options contracts

---

Currently the contracts accept a Uniswap factory address, but do not enforce the existence of a market on Uniswap, that would ensure that options contracts work as intended.

Recommendation
Consider having the factory create an empty market for the token pair.

Follow up [28.08.2020]
The issue was fixed and is no longer present in commit `94bbfb46b769459c28113daa15e4b7a428c79963`.

2. `OptionFactory.sol`: Uniswap and WETH addresses are provided by the user

Both Uniswap and Weth addresses are provided by the user creating the new Option, this allows for bad actors to create markets using rogue versions of Uniswap and/or WETH.

While restricting the underlying and strike assets might not be desirable, Uniswap and WETH addresses will remain constant and could be enforced by the contract.

Recommendation
Use fixed addresses for both the Uniswap Factory and Weth, they can be provided in the Factory deployment, ensuring all options created through the factory will use the intended contracts

Follow up [28.08.2020]
The issue was fixed and is no longer present in commit `94bbfb46b769459c28113daa15e4b7a428c79963`.

3. Beware of malicious tokens

ERC20 implementations come in many forms and some poorly or malicious implemented tokens can break the intended behavior of the contract, making all sorts of attacks possible .It might be especially problematic with tokens that execute code on receiving, like ERC777 or with inflationary/deflationary tokens and other non standard implementations.

Recommendation:
Consider implementing a whitelist of allowed tokens to be used.

Follow up [28.08.2020]
At the contract level any token will be accepted, though a filter of reputable tokens will be produced for the user interface.

Notes

4. `IERC20Mintable.sol`: Interfaces for `approve` and `transfer` are incorrect

Interfaces for both transfer and approve functions do not include the return value (bool).

Recommendation
Consider updating the interface to abide by the ERC20 standard.

Follow up [28.08.2020]
The issue was fixed and is no longer present in commit `94bbfb46b769459c28113daa15e4b7a428c79963`.

5. Consider Using proxies for on-chain deployed contracts

The `OptionFactory` deploys fully functional on-chain contracts, but a cheaper alternative is to use the proxy-master scheme to drastically reduce deploying costs. It does have some drawbacks on readability.

Follow up [28.08.2020]
The team decided to keep the code as is and focus on readability over gas savings. The additional gas costs are restricted to deployments and do not affect ordinary transactions.

6. `PodOption.sol`: Contract could be marked as abstract

If the behavior is to never deploy a standalone `PodOption` contract, consider marking as abstract to make the code more clear.

Follow up [28.08.2020]
The issue was fixed and is no longer present in commit `94bbfb46b769459c28113daa15e4b7a428c79963`.

7. Consider migrating to Uniswap v2

The newer version already has better liquidity as well as increased security with ERC-777 tokens, which are not secure in combination with uniswap v1.

Follow up [28.08.2020]
The issue was fixed and is no longer present in commit `94bbfb46b769459c28113daa15e4b7a428c79963`.

9. Uniswap deadline could be considerably lower

This parameter is used to control how much time a given transaction can stay in the mempool before executing, but in this case, it will always execute within the same block, so the limit could be equal to `block.timestamp + 1`.

Follow up [28.08.2020]
The issue was fixed and is no longer present in commit `94bbfb46b769459c28113daa15e4b7a428c79963`.

10. IPodPut interface does not reflect PodPut

The IPodPut interface does not reflect the interface of PodPut.

Follow up [22.09.2020]
The issue was fixed and is no longer present in commit `2b0f9a5217a6901d17c1e907fe1f0107dd2e86ff`.

Audit Report for Pods on July 28th, 2020.

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of the Pods platform or its products. This audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

Solidified Technologies Inc.