SOLIDIFIED

Audit Report for Clipper DEX - November 18, 2021

Summary

Audit Report prepared by Solidified covering the Clipper DEX smart contracts.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code below. The final debrief took place on November 1, 2021, and the results are presented here.

Audited Files

The source code has been supplied in a private source code repository:

https://github.com/shipyard-software/clipper-rfq-contracts/ (branch: `main`)
Commit number: `f8bfd346c5fface6771eeb4d7305ab659fba0910`

Audited files list:

```
contracts
|-- ClipperDirectExchange.sol
|-- OwnedCollectionContract.sol
```

Intended Behavior

Clipper is a decentralized exchange (DEX) designed to have the lowest per-transaction costs for small-to-medium-sized trades. The current version is an adaptation of the DEX that processes trades of chain and uses the audited contracts for executing swaps, deposit and withdrawal operations pre-calculated off-chain and signed off by the trusted exchange process.

Findings

Smart contract audits are an important step to improve the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of a smart contract system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**.

Note, that high complexity or lower test coverage does not necessarily equate to a higher risk, although certain bugs are more easily detected in unit testing than a security audit and vice versa.

Criteria	Status	Comment
Code complexity	Medium	-
Code readability and clarity	High	-
Level of Documentation	Medium	-
Test Coverage	Medium	-

Issues Found

Solidified found that the Clipper DEX contracts contain no critical issues, no major issues, no minor issue, and 3 informational notes.

We recommend issues are amended, while informational notes are up to the team's discretion, as they refer to best practices.

Issue #	Description	Severity	Status
1	ClipperDirectExchange.sol: Function deposit() redundantly declares a sender parameter	Note	Resolved
2	ClipperDirectExchange.sol: The contract has no token escape function	Note	Acknowledged
3	ClipperDirectExchange.sol / WrapperProxy.sol: Functions transmitAndDeposit() and transmitAndSwap() do not follow standard naming conventions	Note	Acknowledged

Critical Issues

No critical issues have been found

Major Issues

No critical issues have been found

Minor Issues

No minor issues have been found

Informational Notes

1. ClipperDirectExchange.sol: Function deposit() redundantly declares a sender parameter

Function `deposit()` always reverts if `sender` is not equal to `msg.sender`, which effectively makes sending an additional `sender` parameter redundant.

Recommendation
Remove the `sender` parameter and always use `msg.sender` instead.

Status
Resolved

2. ClipperDirectExchange.sol: The contract has no token escape function

---

Recommendation

Consider adding a token escape function in case a user accidentally sends a token that is not present in `assetSet`.

Status

Acknowledged

3. ClipperDirectExchange.sol / WrapperProxy.sol: Functions transmitAndDeposit() and transmitAndSwap() do not follow standard naming conventions

---

Recommendation

Consider renaming the functions to `transferAndDeposit()` and `transferAndSwap()`, respectively.

Status

Acknowledged

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Clipper DEX 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.