Abstract

For this audit, client has engaged us to review a single Clarity contract (btc-stx-swap.clar). The contract, as titled, is a swap engine for a single trading pair: STX <> BTC (L1).

The design is made with two key data maps (swaps & swap-offers) with the following life-cycle:

1. Collateralize Swap
2. Set Swap Price
3. Two paths here:
    a. Reserve Swap
    b. Submit Offer -> Accept Offer
4. Submit Swap | Submit Swap SegWit

In short, once collateralized & priced by the seller (putting up STX in exchange for BTC), it's on the buyer to either reserve the swap as priced or they submit a swap offer. If reserved, the buyer/reserver must submit a swap proof to receive their STX; if a swap offer is made, the seller must accept an offer & then the buyer submits a proof.

Contract Outline					
Name	**Type**	**Call?**	**Priv**	**Pub**	**Read**
btc-stx-swap	core	12	1	10	3

Findings

Below is a summary & list of all priority (0-3) issues found throughout an independent or paired review session. P0s have a high certainty in loss of protocol | user funds, P1s have a low probability through events such as admin accidents | governance exploits, P2s are highly recommend & p3 issues are optional (usually syntax/optimization based)

<u>As of now, with a p1, we cannot recommend this protocol launch until at least this severe issue is amended.</u>

(p1) Permanent Reserve Can Grief A Swap *presented*
suggestion(s)

The suggestion here would be to optimize to cause Alice to take zero additional option if a reservation expires. Therefore, a solid solution here could be:

1. Adding a “expired-height”:uint value in the swaps map
2. Deciding on an expiration height (I suppose this could just be the existing 6-block wait period)
3. Update affected functions such as submitting another reserve
4. Remove the existing reserve check in the swap offers since the seller should commit offers regardless so that they can accept one as soon as reservation expires

(p3) Incorrect Error Numbering *presented*

One error is numbered all the way up at u99 for unclear reasons.

suggestion(s)

Update to correct numbering.

(p3) Lack of Comments *presented*

There are very few useful comments. The readability could be drastically improved here.

suggestion(s)

Add meaningful comments to every core function.