Gamma BTC STX Swap Light Audit

Gecko Security

August 2024

Overview

The BTC-STX Swap contract was audited focusing on its security and correctness. The audit covered key functionalities, including swap creation, bid/ask mechanisms, collateral management, and Bitcoin transaction verification. The focus was to ensure the contract operated as intended in edge cases and was free of potential vulnerabilities.

Methodology

The audit process involved:

1. **Code review:** Thorough examination of the contract code, focusing on logic, security, and adherence to best practices.
2. **Functional testing:** Verification of all key functions using Clarigen for simulating various scenarios.
3. **Edge case analysis:** Identifying and testing potential edge cases and unusual scenarios.
4. **Comparison with previous audit:** Reviewing changes and improvements since the last audit.

Key Areas Audited

1. **Swap Functions**
    a. Verified the new functionality allowing BTC senders to place bids before STX swap creation and collateralization.
    b. Tested scenarios where BTC senders bid with lower uSTX amounts than the collateralized amount.
    c. Confirmed correct matching of asks and bids without errors.
2. **Cancellation Functions**
    a. Validated state transitions to ensure actions like taking an ask are correctly blocked after cancellation.
    b. Tested the claim-collateral function to ensure proper STX return to the sender in all valid cancellation scenarios.
    c. Verified the combined cancel-all-and-claim function fully resets the swap state and deletes the swap as expected.
3. **BTC Transaction Verification**
    a. Tested mechanisms to prevent double spending, confirming that the same Bitcoin transaction cannot be reused in multiple swaps.
    b. Analysed the cooldown period implementation to mitigate risks associated with Bitcoin network reorganisations.
4. **Access Control**
    a. Verified that unauthorised attempts to modify or submit transactions are properly blocked.
    b. Confirmed that only appropriate principals can execute specific functions.
5. **Front-Running Protection**
    a. Simulated the contract's reliance on block height for cooldown periods and expiration times with upcoming faster block times to ensure front-running protection.

6. **Collateral Management**
    a. Verified correct locking of STX collateral during swap creation and appropriate release under various conditions.
    b. Confirmed that collateral is never released prematurely or under inappropriate circumstances.
7. **Fee Management**
    a. Analysed the flexible fee contract selection and its implications.
    b. Tested scenarios with malicious fee contracts and tokens to assess potential risks.
8. **New Features and Changes**
    a. Audited the implementation of the premium as a penalty recouped when the swap happens, ensuring compliance with regulatory considerations.
    b. Verified the functionality of cancel-ask, cancel-swap, cancel-swap-and-ask, and cancel-all-and-claim functions.
    c. Confirmed that the expiry and cooldown periods work as intended and cannot be manipulated through block time manipulation.

Improvements Since Previous Audit

1. The P1 issue of permanent reserve griefing a swap has been mitigated through the implementation of expiration heights and more flexible cancellation options.

Current Findings

1. The implementation of bidding before swap creation introduces additional complexity but appears to be handled correctly.
2. The cooldown period mitigates swap risks from Bitcoin network reorganizations, but doesn't prevent premature Bitcoin sending. This limitation could invalidate STX collateral if a reorganization occurs, necessitating robust user education.
3. The new cancellation functions provide more flexibility in managing swaps but increase the complexity of the contract's state management (shown in Clarigen Testing).

Recommendations

1. Consider implementing a whitelist or verification mechanism for fee contracts to further mitigate risks associated with malicious fee contracts.

Conclusion

The BTC-STX Swap contract has addressed all previously identified high issues and is now deemed suitable for mainnet deployment. All exploitable risks have been mitigated, with any remaining risks assessed as low and insignificant.