Ana Tatabitovska , 4842324, Research Project - CSE3000, a.tatabitovska@student.tudelft.nl

Oğuzan Ersoy, Zekeriya Erkin

Mitigation of Transaction Manipulation Attacks in UniSwap

Key Definitions

- Decentralized Finance systems
- UniSwap
- Transaction manipulation attacks

Question

How can UniSwap protect itself from transaction manipulation attacks and to what extent would a possible solution impact its current modus operandi?

Analysis

Factors which contribute to transaction manipulation attacks:

1. Slippage - manner in which attackers profit off of users
2. Miners in Validation Protocols - actors that can be bribed to reorder transactions
3. Privacy - lack of transaction encryption offers attackers privilege to sensitive information

Attacks in UniSwap

1. Moving the Market Against the Trader
2. Sandwich with Mint and Burn

Solution: Submarine Commit

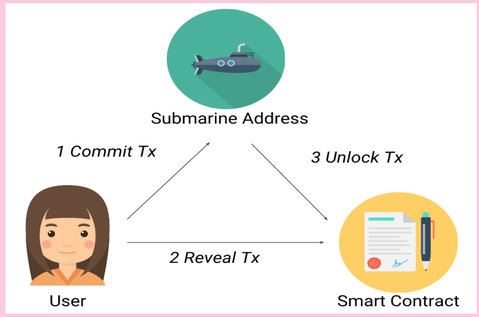

Figure 1: Submarine Commit, adapted from libsubmarineorg [1]

Modification for UniSwap:

- Each Pool in UniSwap is able to verify a reveal and gather data
- Deposit for Commit-Reveal scheme calculated using slippage caused by intended transaction rather than bounty value

Time Lock Scheme

Lock users from performing actions in a pool after a mint transaction for a period of time

Off-chain Slippage

User-set limit on maximum tolerated slippage per transaction

Conclusion & References

Both mitigations are imperfect and create a strain in the UniSwap protocol
Transaction manipulation attacks shoul be solved at the blockchain level

References
[1] “Defeat Front-Running on Ethereum,” libsubmarine.org. [Online]. Available: https://libsubmarine.org/. [Accessed: 29-Jun-2021].

Figure 2: Ethereum workflow (own work)