By: Akif Yüksel (4878868)
E-mail: a.a.yuksel@student.tudelft.nl
Supervisor: Oğuzhan Ersoy
Responsible professor: Zekeriya Erkin
Examiner: Julian Urbano
Date: July 1st, 2021

CSE 3000 – Research Project

Sandwich attacks in Kyber DMM

TU Delft Delft University of Technology

1. Background

- Kyber Network – on-chain liquidity protocol
- Kyber DMM – an upgrade to the existing AMM, mitigates Capital Inefficiency (CI) by means of an amplification factor a
- Virtual reserve: $ax \cdot ay = a^2k$ as opposed to $x \cdot y = k$ in Uniswap v1

2. Research Question

How can one mitigate the vulnerability for sandwich attacks in Kyber DMM?

3. Methodology

- Literature study – (white)papers, security audits and Kyber's blog
- Implementation – modify existing test case in DMM GitHub repo

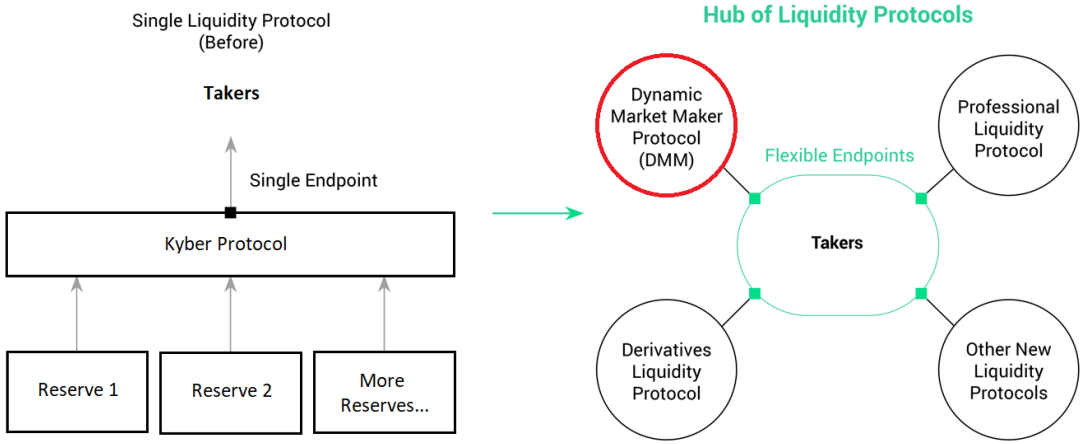

Figure 1: Kyber 3.0: upgrade from single liquidity protocol to hub of liquidity protocols

From: https://blog.kyber.network/kyber-3-0-architecture-revamp-dynamic-mm-and-knc-migration-proposal-acae41046513

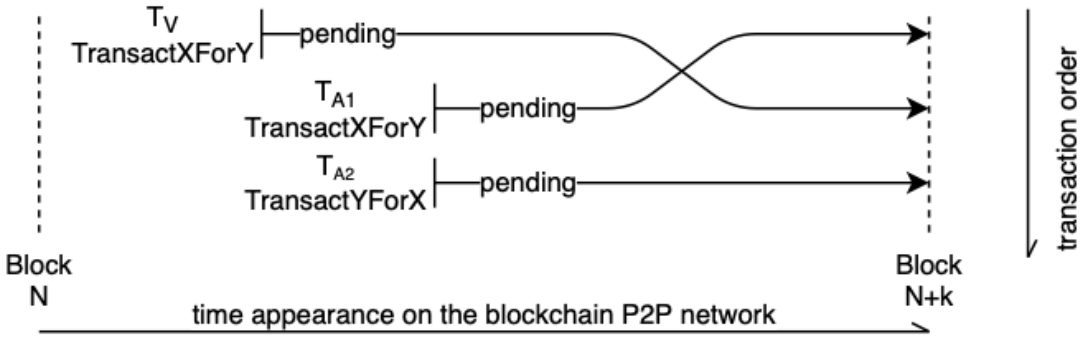

Figure 2: General structure of a sandwich attack.

from Zhou, L., Qin, K., Torres, C. F., Le, D. V., & Gervais, A. (2020). High-Frequency Trading on Decentralized On-Chain Exchanges. arXiv preprint arXiv:2009.14021.

4. Problem

- "Sandwiching" a real transaction
- Virtual reserve ratio unbalanced
- Amplification factor of 100x leads to loss of 12.69% for victim

5. Mitigation

- Current mitigation: Slippage protection in the router
- Verifying vulnerability is present
- Suggestion: broaden mitigation by correcting pool contract

6. Conclusion

- Mitigations in literature unrealistic
- Security vulnerability in pool contract not mitigated
- Suggestion to implement similar code correction in pool contract