Associate Professorship of Embedded Systems and Internet of Things
Department of Electrical and Computer Engineering
Technical University of Munich

Are Smart Contract Attack Strategies Optimized?

Bachelor Thesis

Jens Ernstberger, November 15, 2022

Title: "Are Smart Contract Attack Strategies Optimized?"
Supervisor: Jens Ernstberger, Liyi Zhou
Period: 12 weeks

Description

Blockchain-based Decentralized Finance (DeFi) ecosystem has attracted a surge in popularity since the beginning of 2020. The peak total value locked (TVL) for DeFi surpassed 253 billion USD on Dec 2, 2021, with Ethereum (145 billion, 57% TVL) and BNB Smart Chain (19.8 billion, 8% TVL) sharing the majority of DeFi's activity. While DeFi certainly provides many protocols inspired by traditional finance such as cryptocurrency exchanges, lending platforms, and derivatives, novel constructs known as flash loans and atomic composable DeFi trading emerged. Unfortunately, these very intertwined DeFi systems, coupled with the already well-studied vulnerability-prone smart contracts, broadened the threat surface of DeFi protocols. However, recent work [1] shows that attacker strategies are far from optimal. Attacks are not executed atomically, and attackers leave potential extractable value in exploitable contracts due to non-optimized attack strategies.
In this thesis, you should evaluate whether attack strategies change over time, and whether attackers react to recent findings. To do so, you need to extend an existing dataset based on a pre-defined methodology in a first step. Based on the newly added incidents and attacks, you should evaluate at least the following [1]: *(i)* whether the rescue time-frame shrinks; *(ii)* whether attackers still broadcast their transactions on the public P2P network; and *(iii)* whether attacks are sub-optimal, which emits profitable trading opportunities that are extracted by benign arbitrageurs. In addition, you should further propose metrics that quantify the change in attackers' behavior.

Tasks

The thesis is separated into several working packages.

1. Introduction: Get familiar with Ethereum, EVM and the existing dataset.
2. Data Collection: Update the dataset to obtain data that enables the evaluation of attacker strategies.
3. Analysis: *(i)* whether the rescue-timeframe shrinks; *(ii)* whether attackers use private relayers more frequently; and *(iii)* whether attacks still emit arbitrage opportunities.
4. Further Metrics: Propose further metrics that allow the evalaluation of a change in an attackers strategy.
5. Evaluation: Evaluate your porposed metrics to see whether a change in attacker strategy occurs.
6. Report: Write the report.

Preliminary Schedule

Task / Week	1	2	3	4	5	6	7	8	9	10	11	12
Introduction												
Data Collection												
Analysis												
Further Metrics												
Evaluation												
Report												

References

[1] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "Sok: Decentralized finance (defi) incidents," *arXiv preprint arXiv:2208.13035*, 2022.