AGENT-BASED MODELING FOR BLOCKCHAIN AUTOMATED MARKET MAKER AND ECONOMIC APPLICATIONS

Ziqiao Ao

Data Science | Signature Work Class of 2022

Introduction

Trading through automated market makers (AMMs) on Ethereum is gaining a significant tendency in Decentralized finance (DeFi). However, the mechanism of slippage tolerance set by trades in AMM offers opportunities for predatory trading bots to gain extra profits by conducting invisible sandwich attacks. Considering that few studies have been conducted to investigate the trading behavior within the attack from a micro perspective, our study proposed an agent-based model to simulate the sandwich game to evaluate how different players would perform under the predate, especially when trading Uniswap. We adopt Heimbach et al.'s (2022) model, which could automatically adjust traders' slippage tolerance to minimize costs instead of using the initially fixed slippage set in the AMM. Moreover, we further revise the model by adding other kinds of behavioral players considering bounded rationality. We demonstrate the impact of bounded rationality on trading behaviors concerning the trading loss. This study would provide a micro foundation for the macro context, specifically the DeFi token transaction network structure, and economic performance evolution. The novel application scenarios and proposed modeling methods would greatly inspire future research on agent-based modeling for the cryptocurrency market for more complex environments.

Materials and Methods

Agent-based modelling is adopted in this study to simulate the sandwich attack when trading between Aave and Ether under Uniswap Automated market maker. In particular, we would like to:

1) Replicate the model proposed by Heimbach et al. (2022), that is to simulate the sandwich game, which formalizes the sandwich attack problem from both the trader's and the bot's perspectives, which could automatically adjust traders' slippage tolerance to minimize costs instead of using the originally fixed slippage set in the AMM;
2) Based on bounded rationality, besides the rational players who are expected to minimize costs, we will assume another kind of behavioral player who could not achieve this purpose due to different kinds of cognitive limitations for comparison.

昆山杜克大学
DUKE KUNSHAN UNIVERSITY

To estimate and evaluate the parameter setting of the proposed model, we acquire the real data of all Uniswap V2 transactions recorded on Ethereum under centrain blocks to find the optimal simulation that could explain the reality.

Results

1. Sandwich Game

```
'''
input:
s: sllipage tolerance
f: transaction fee, 0<=f<1
b: base fee per transaction
X0_reserve: token X reserved in the liquidity pool at time t0
y0_reserve: token Y reserved in the liquidity pool at time t0
X_paid > 0: tokens X entering the mempool at time t0;
X_a >0: token X charged when predatory bot first executes a transaction TA1

output:
P_a: bot profits
'''
```

2. Adversary Perspective

Finding the optimal attack input X_a that maximizing Profits

```
'''
input:
s: sllipage tolerance
f: transaction fee, 0<=f<1
b: base fee per transaction
X0_reserve: token X reserved in the liquidity pool at time t0
y0_reserve: token Y reserved in the liquidity pool at time t0
X_paid > 0: tokens X entering the mempool at time t0;

output:
X_a: optimal attack input for bots
'''
```

3. Trader Perspective

Finding the optimal slippage tolerance that minimizing the trader's cost

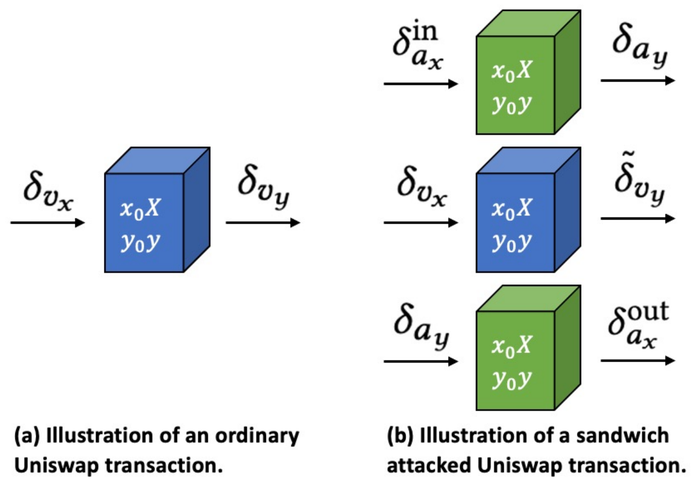
```
'''
input:
f: transaction fee, 0<=f<1
b: base fee per transaction
X0_reserve: token X reserved in the liquidity pool at time t0
y0_reserve: token Y reserved in the liquidity pool at time t0
X_paid > 0: tokens X entering the mempool at time t0;

output:
s: optimal slippage tolerance
'''
```

For transaction $T_v = (\delta_{v_x}, s, f, b, x_0, y_0, t_0)$ in pool $X \rightleftharpoons Y$

Calculate $s_a = \frac{2b}{\delta_{v_y}}$ and $s_r = \frac{p(s,\delta_{v_x})}{1-p(s,\delta_{v_x})}\left(\frac{(l+m)b}{\delta_{v_y}} + \mathbb{E}(s|\tilde{s} > s)\right)$ for transaction T_v

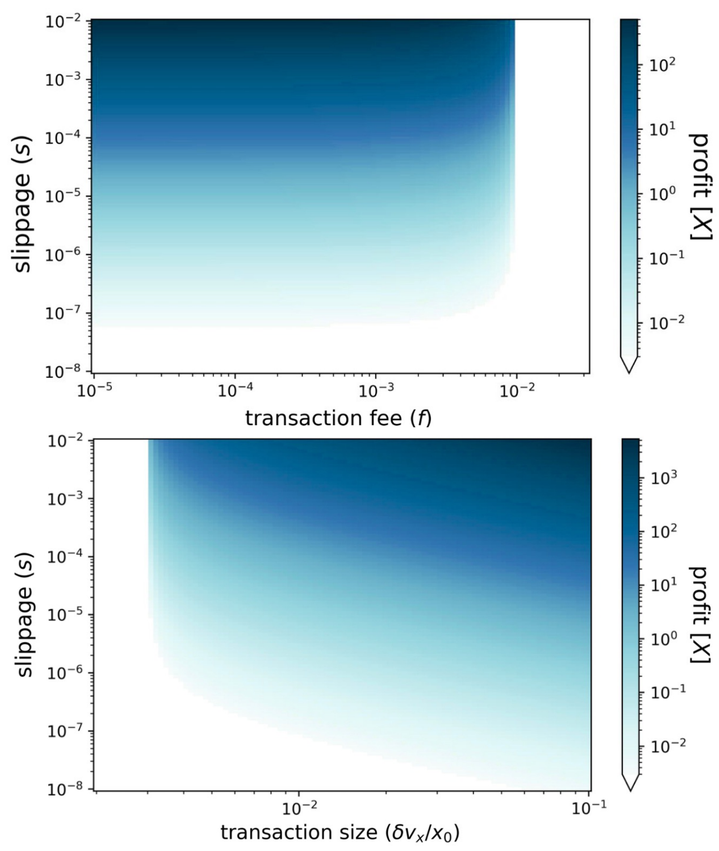
if $s_r < s_a$:
    set $s = s = s_a - \varepsilon$, where $\varepsilon \to 0^+$
else:
    set $s = s_r$

Visual



(a) Illustration of an ordinary Uniswap transaction.

(b) Illustration of a sandwich attacked Uniswap transaction.



Discussion

Because this model is a new attempt in DeFi applications, the assumptions and parameter settings of the model could be further optimized by considering more potential, significant effects. We could extend our agent-based model to multi-agent reinforcement learning for future research, which could consider more complex conditions and automatically find the optimal parameters with higher accuracy. The multi-agent reinforcement learning model has been applied in the traditional financial market (Lussange et al. 2021 and Liu et al. 2020), while few in the cryptocurrency market. Therefore, our potential future research will also be of great contribution and significance.

Based on our proposed model, others would evaluate different DeFi token trading strategies on AMM and behaviors of traders by comparing the profits gained. They could also adapt this model to other scenarios such as the stock market, ETH, and Bitcoin transaction market to assess how the interaction between different players would affect network structure and economic performance. The agent-based modeling methodology could also be applied to solve real-world issues in industry fields. Further, such a bottom-up study could be extended from micro modeling to more macro policymaking as we found the effects of trading patterns on the economy.

Conclusion

In this study, we extend the sandwich attack problem to include multiple types of traders and predatory bots. Our study shows that, by retuning the algorithm proposed by Heimbach et al. 's (2022), rational traders defined under the optimal model can easily avoid most sandwich attacks by adjusting their slippage tolerance and do not face unnecessarily high risk of trade failure, and their consumption was reduced by automatic sliding better than Uniswap's recommendation of fixed settings. However, given the bounded rationality, we hypothesized and proved by modelling that behavioral and random traders are more vulnerable to sandwich attacks than rational traders, which is in fact unavoidable. In any case, this would provide an opportunity for AMM itself or a new DeFi service to guarantee a given (low) slip fault tolerance for users by apportioning the cost of the user pool.

However, although our model assumes a variety of traders, the actual trading network is often more complex. We hope to adopt social network analysis to analyze the trading network in future studies, extract more complex trader behaviors and bring them into AMM transactions, especially sandwich attack scenarios. To develop more advanced methods to prevent more predatory trading practices.