Agent-Based Modeling for Blockchain Automated Market Maker and Economic Applications

Signature Work Final Report

Ziqiao Ao, Data Science, Class of 2022, Duke Kunshan University
Supervisor: Prof. Luyao Zhang, Duke Kunshan University

Keywords:[Decentralized finance], [Agent-based modeling], [Sandwich Attack], [Bounded rationality], [Mechanism design], [Automated Market Maker]

Acknowledgments:
Throughout the whole project and the writing of this dissertation, I have received a great deal of support and assistance.

I would first like to thank my supervisor, Professor Luyao Zhang, whose professional theoretical knowledge and rich experience offered me valuable help and guidance in determining research problems and methods. Whether from Economics or Data Science, you have promoted my research to a higher level and more in-depth insight.

I would like to acknowledge Professor Gergely Horvath; the key guiding advice and forward-looking ideas make my research have a lasting significance.

NetID:[za36]
Contact: [za36@duke.edu]
Last Update: [Mar 27, 2022]
Google Folder:
[https://drive.google.com/drive/folders/1p1SpWc6qd-mA55zQe3w2JVf7gemeTTlC?usp=sharing]
Mybib Folder: [https://www.mybib.com/j/InexpensiveDidacticRail]

Research Summary

Abstract:

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 investigated 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.

Table of Contents

Part I: Research Description

1. Introduction

1.1 Background and Motivation

With the emergence of Decentralized Finance (DeFi) and the popularity of various DeFi products, more and more research on the decentralized market and cryptocurrency trading. Scholars and practitioners are very concerned about whether decentralization is a good feature of the blockchain market so that more fit-for-purpose policies could be assessed and made correspondingly. However, the dependence of smart contracts on automated market makers on DeFi for transaction sequencing has led to the prevalence of sandwich attacks on DEX transactions, which have resulted in numerous transactions being entrapped and earning intermediate profits, and in which different types of trading behavior can result in different levels of loss. To evaluate, studies will be conducted from macro and micro perspectives. Some existing studies demonstrated that network measures could affect the cryptocurrency market's price and other economic features from a macro perspective. (Motamed and Bahrak 2019, Vallarano, Tessone, and Squartini 2020 and Bovet et al. 2019). However, few studies have been conducted to investigate the trading behavior from a micro perspective. Cocco, Tonelli, and Marchesi (2015 & 2019) proposed two models that simulate the Bitcoin trading process to reproduce the market's main characteristics and trading profits, respectively, but they are not comprehensive enough and cannot be directly applied DeFi applications. Specifically, Heimbach and Wattenhofer (2022) proposed a novel agent-based model to simulate the sandwich game, which formalizes the sandwich attack problem from both the trader's and the bot's perspectives, and could automatically adjust traders' slippage tolerance to minimize costs instead of using the fixed initially slippage set in the AMM. However, they fail to consider the bounded rationality of traders and neglect those behavioral and irrational traders.

1.2 Research Questions

Based on the accomplishments and limitations of existing studies, the research question of this study comes to be:

1. What optimal strategies for rational traders under sandwich attacks to minimize their costs?
2. How will the trading behaviors of traders affect their costs under sandwich attack?

As the DeFi field has newly emerged, relevant research is not very comprehensive and in-depth enough, so this question has not been answered yet. In order to answer this question, we would utilize a bottom-up approach by proposing an agent-based model, which relies on the bounded rationality theory to define different types of traders, to simulate the sandwich attack of the transaction between Aave and Ether under Uniswap. We will use real market and transaction data to assess the model and compare the influence. This study would contribute to the existing literature since it would provide a micro foundation for the macro context, specifically the DeFi transaction under automated market maker and risk management. 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.

2. Literature Review

Our research contributes to the literature on the interplay of decentralized banking, automated market maker, sandwich attack, bounded rationality, and agent-based modeling.

1. We dived into a micro investigation into how different traders interact to affect the transaction network and outcomes.
2. Instead of focusing on the macro contexts to conduct data analysis methodology utilizing the historical data to study the relationship and causality, we provided a micro foundation by proposing an agent-based model to simulate the trading process under such macro contexts, which could add dimension to the study the main characteristics and effect of the real market.
3. Besides simulating the optimal strategies for rational agents under sandwich attacks (Heimbach et al. 2022), we assume some other types of behavioral agents besides rational ones into the model for comparison and testing the efficiency of the previously proposed model.
4. By adapting the agent-based model based on the bounded rationality theory to the Aave token transaction, we apply the traditional theory and methodology to a novel area, which is decentralized finance.

Since few agent-based models are used in the cryptocurrency market, our study would make significant innovations and breakthroughs and has excellent application possibilities in the broader DeFi economy and the cryptocurrency market in the future. The following parts will summarize existing literature introducing decentralization banking, automated market maker, sandwich attack, bounded rationality, and agent-based modeling.

Decentralized Bank and AAVE

DeFi, short for decentralized finance, is a blockchain-powered peer-to-peer financial system that incorporates financial applications in blockchain and cryptocurrency (Werner et al., 2021). It is limited to simple value transfer and expands to more complex economic use cases. DeFi could disrupt centralized finance, centralized exchanges, and centralized banking by lowering

transaction costs and enabling users to interact with peers (Harvey, Ramachandran, and Santoro 2021) directly. Most DeFi applications are built on Ethereum due to its smart contracts mechanism. Decentralized exchanges are gaining popularity as they allow latent liquidity observation and form a distributed peer-to-peer network (Lehar and Parlour, 2021).

Crypto tokens are digital assets that utilize blockchain and cryptography technology to ensure security (Halaburda et al., 2022). As of Jan. 20, 2022, the market value of crypto tokens is beyond 1.9 trillion U.S. dollars. Cong and Xiao (2021) categorize cryptocurrencies into general security, utility (general payment and platform), and product tokens based on functions. Bitcoin, the first cryptocurrency, is designed as a transaction mechanism and classified as utility (general payments) tokens. Though Bitcoin dominated the market between 2009 and 2016, other alternatives emerged later (Härdle, Harvey, and Reule 2020). Ethereum blockchain revolutionized in supporting smart contracts to allow automatic transactions and issuing ERC (Ethereum Request for Comments) tokens. (Liang, Li, and Zeng 2018; Lehar and Parlour 2021).

Our research studies the transaction between Aave and Ether. Aave, ranked top among DeFi products, is a decentralized liquidity market protocol that serves as a non-custodial platform where users could participate as depositors or borrowers. The market value of Aave is beyond 2.9 billion U.S. dollars as of Jan. 20, 2022 (coinmarketcap 2022). Aave is a decentralized bank that allows users to lend and borrow crypto assets and earn interests on assets supplied to the protocol. (Whitepaper.io 2020) In general, decentralized banks differ from centralized banks in two aspects: 1) replace centralized credit assessments with coded collateral evaluation (Gudgeon et al., 2020); 2) employ smart contracts to execute assets management automatically (Bartoletti et al., 2021). The open-source codes of the decentralized bank: Aave, and the transparent trading data of the AAVE token enable us to reproduce the historical network dynamics.

Uniswap and Automated Market Maker

Automated market maker on Uniswap, a decentralized exchange for transactions between Aave and Ether. Automated market makers (AMM), first introduced by Hanson's logarithmic market scoring rule (LMSR) (Hanson 2003), are contracts that allow providing liquidity to the crypto

market automatically (Fritsch and Zürich 2021), it allows automatic trading of cryptocurrencies by an algorithm. Uniswap utilizes a constant product market maker (CPMM). CPMM ensures that the product between the two reserved pool currency amounts remains constant. Based on the AMM, this contract is built on Uniswap, allows agents to trade between Aave and Ether at the price and rates specified by the pricing function, and the price will be kept updating for each trade (Angeris et al. 2020). Our research studies the transaction between Aave and Ether under the Uniswap AMM.

Sandwich attack

Sandwich attacks involve victim trades running in the front and back office by forcing trades to be executed at unfavorable prices and then taxing the victim's trades by exploiting the resulting price differences (Heimbach and Wattenhofer 2022). Uniswap's AMM automatically suggests to traders a fixed slippage tolerance, i.e., the maximum acceptable price movement. However, this fixed setting is not flexible enough to adjust to changes in other parameters of the trade and therefore does not give the trader consistently good attack avoidance and exertion control.

There are three types of players in the sandwich game: traders, predatory trading bots, and miners. Traders initiate DEX trades to mempool, which can turn into potential bait for predatory trading bots. Predatory trading bots listen to these incoming trades and launch sandwich attacks if they deem them profitable: aimed at front- and back-office manipulation of traders' trades. Finally, miners select and order trades from mempool in a block.

The sandwich game simulation model proposed by Heimbach and Wattenhofer (2022) formally mentions the analysis of sandwich attacks from the perspective of traders and bots. Traders indicate their slippage tolerance - the maximum acceptable price movement. The slippage mentioned above tolerance simultaneously generates the sandwich attack: the front and back victim trade. Predatory traders listen to the mempool trades and attack those that present a profit opportunity. In general, the profitability of the sandwich attack increases with the size of the victim's trade and the slippage tolerance. Heimbach and Wattenhofer (2022) proposed a model

that contributes to the sandwich game by automatically adjusting traders' slippage tolerance to minimize costs instead of using the originally fixed slippage set in the AMM.

Bounded rationality and mechanism design

Bounded rationality is often utilized to define rational choice that considers the decision maker's cognitive limitations, referring to knowledge and computational capacity limitations (Simon 1990). Cognitive limitations are limited to specific information and the adequacy of scientific theories that can be used to predict related phenomena, for instance. Instead of assuming known probability distributions for outcomes, we need to estimate their programs or find strategies for dealing with uncertainty that does not assume probabilistic knowledge. Instead of maximizing the utility function, we must assume a sound strategy based on different conditions(Clippel and Rozen, 2021). Bounded rationality more ambitiously captures the actual decision-making process and the essence of the final decision itself. Such credible theories can only be based on empirical knowledge of the capabilities and limitations of the human mind, depending on the situation.

Bounded rationality could be observed in the cryptocurrency market. Due to the cognitive limits, not all traders are rational ones who constantly seek to maximize their profits. Therefore, we have another type of trader to define in this market: the behavioral trader. Due to their lack of understanding of the DeFi market, or investment theories and methods, they cannot maximize profits, nor are they necessarily aiming to maximize profits. This group of people could be defined as random players - who behave in a random walk, market disrupters, or bandwagons (Koens, Van Aubel, and Poll 2020). These two types of traders would interact, bringing different effects to the whole transaction network, degree of decentralization, and economic performance, which could only be investigated based on the micro foundation of bounded rationality theory through a simulation process. (more literature to define players)

Agent-based Modeling

An agent-based model (ABM) is a computational model that can simulate the actions and interactions of individuals and organizations in complex and realistic ways, which could provide precious information and insights into the complex dynamics and characteristics of the real-world system. Agent-based models are not constrained by many of the constraints and empirical problem assumptions of most mainstream economic models (Iori and Porter 2012).

Therefore, applying ABM to simulate the economic markets with many interacting agents shows increasing promise in research that could greatly influence how we think about micro-interactions in economic models and their impact on economic performance. In this field, the financial market is deemed as an important application scenario for agent-based modeling due to the characteristics of 1) agents having clear objectives, 2) easy accessibility to the corresponding data, and 3) possibilities to make comparisons by controlling the conditions in agent-based experiments (LeBaron 2000).

Compared with the traditional financial market, fewer works have been made to model cryptocurrency markets; Cocco, Concas, and Marchesi (2015) proposed a complex agent-based model to study the cryptocurrency market and capture the main characteristics of the market. Their model incorporates two agents, Random Traders and Chartists, which interact in the transaction network by trading Bitcoins, based on previous simulated financial market models; According to her strategy and resources, each agent is initially endowed with a finite amount of crypto, fiat cash and issues buy and sell orders. The model proposed can reproduce the unit root property, the fat tail phenomenon, and the volatility clustering of the Bitcoin market. However, this study failed to consider the interplay between different cryptocurrencies or the network structure and effects among traders.

Cocco, Tonelli, and Marchesi (2019) later developed another agent-based model to simulate Bitcoin trading and reproduce the main characteristics of the Bitcoin market by implementing different trading strategies and price clearing mechanisms based on real order books. They still incorporate Chartists and Random traders to perform trading in this model. Chartists apply trading rules that expect to maximize profits, and rules with randomly-selected parameters constitute the other. The results further show that the Chartists who adopt the best trading rules

can always achieve higher profits than the other type. However, in this model, since they only implement the model through the genetic algorithm due to the computational complexity, they only consider buying and selling orders of a single amount. For each buys or sells order issued, the system automatically generates a sell or sell-buy order.

3. Methodology

3. Model

Agent-based modeling 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; and 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.

In the following paragraphs, we will first introduce the transaction and attack model in general, then the Heimbach et al.'s (2022) sandwich game model in detail, and last introduce our adaption and revise the model considering bounded rationality.

There are three types of players in the sandwich game: traders, predatory trading bots, and miners. In our study, we assume that the predatory trading bots are miners themselves, which could allow them to order their transactions around the trader's transaction without extra cost strategically.

3.1 Transaction model in Uniswap

From the trade perspective, for a transaction between token *X* and token *Y* in Uniswap, we consider the liquidity pool $X \rightleftharpoons Y$ with reservesx_0 and y_0 at the time t_0, respectively. The current base fee, which is defined as the minimum fee per gas in general, is used as the minimum fee per Uniswap transaction in our model, denoted by *b*, considering that all individual Unisawp V2 transactions ask for approximately the same amount of gas.

A transaction T_v entering the mempool at the time t_0 that trades by exchanging δ_x the amount of token *X* for δ_{v_y} token *Y* is defined as $T_v = (\delta_{v_x}, s, f, b, x_0, y_o, t_0)$, where s gives the slippage tolerance, f and b are the transaction fee and base fee respectively. We have

$$\delta_{v_y} = y_0 - \frac{x_0 \cdot y_0}{x_0 + (1-f)\delta_x} = \frac{y_0 (1-f)\delta_x}{x_0 + (1-f)\delta_x}$$

However since the transaction might not always execute exactly at the time t_0, then if we suppose it is executed at time t_1, then this trade will output

$$\overline{\delta}_{v_y} = \frac{y_1 (1-f)\delta_x}{x_1 + (1-f)\delta_x}$$

amount of token *Y*. Based on the changes in the pool reserves between time t_0 and t_1, the trader might receive more or fewer tokens *Y*. To prevent the exchange rate from falling significantly due to the time difference, the slippage tolerance *s* specified by AMM would only allow the trade only to execute at the time t_1 if

$$\overline{\delta}_{v_y} \geq (1 - s)\delta_{v_y}$$

or the trade will fail to execute otherwise.

3.2 Attack Model

The predatory trading bot listens to the inflowing transactions in the mempool.
When the trade $T_v = (\delta_{v_x}, s, f, b, x_0, y_o, t_0)$ enters the mempool, the predatory bot will compute the optimal input δ_{a_x} for the sandwich attack based on the attack profits.

We assume optimal conditions for the predatory trading bot: access to unlimited funds, guaranteed transaction ordering, and only paying the base fee. Assuming that the predatory trading bot has access to unlimited funds is reasonable and represents the worst case for traders. Additionally, letting the miner be the predatory trading bot again represents the worst case for

traders. Further, it allows the trading bot to only pay the base fee for its transactions and control transaction ordering. We further assume that the trading bot takes the front-running transaction's output as the input of the back-running transaction.

3.3 Sandwich Game

The entire sandwich game process would be divided into three parts: 1) the general mechanism of the game, 2) optimal attack input finding from the predatory perspective, and 3) optimal slippage tolerance finding from the trader's perspective.

3.3.1 General game mechanism

Here we first start with the general mechanism of the game. Transaction $T_v = (\delta_{v_x}, s, f, b, x_0, y_o, t_0)$ at the time t_0 must satisfy conditions that $\delta_{v_x} > 0$ in pool $X \rightleftharpoons Y$, the reserves token $x_0 > 0$ and $y_o > 0$, the pool transaction fee should be $0 \leq f < 1$, and the slippage tolerance is $0 < s < 1$. Then, if the reserves in the pool perform no change at the time t_0, the trader is expected to receive δ_{v_y} token Y with

$$\delta_{v_y} = \frac{y_0(1-f)\delta_x}{x_0+(1-f)\delta_x},$$

Nevertheless, if a sandwich attack happens in the meantime, the predatory bot will first execute a transaction T_{A_1} by exchanging $\delta_{a_x}^{in} > 0$ token X for δ_{a_y} token Y with

$$\delta_{a_y} = \frac{y_0(1-f)\delta_{a_x}^{in}}{x_0+(1-f)\delta_{a_x}^{in}},$$

In this situation, the trader transaction will execute at a time t_1, with reserves $x_1 = x_0 + \delta_{a_x}^{in}$, and $y_1 = \frac{x_0 \cdot y_0}{x_0+(1-f)\delta_{a_x}^{in}}$, the trader can only receive

$$\bar{\delta}_{v_y} = \frac{y_1(1-f)\delta_{v_x}}{x_1+(1-f)\delta_{v_x}} = \frac{\frac{x_0 \cdot y_0}{x_0+\delta^{in}_{a_x}}(1-f)\delta_{v_x}}{x_0+\delta^{in}_{a_x}+(1-f)\delta_{v_x}} < \delta_{v_y}$$

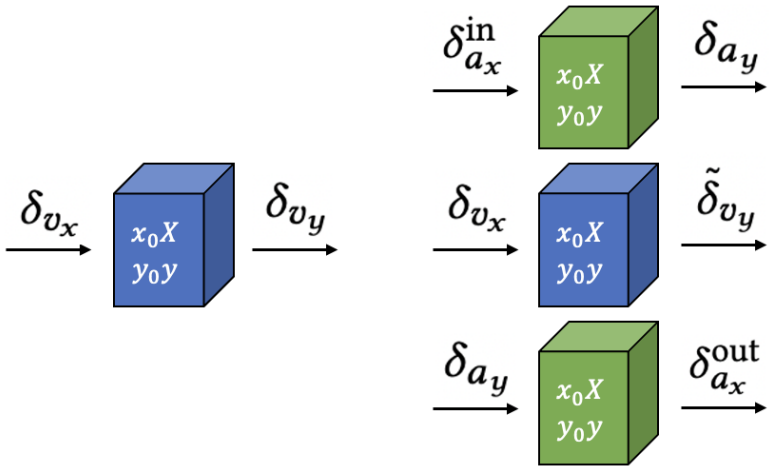
token Y. Then, the predatory bot finishes the attack by exchanging δ_{a_y} at a time t_2 with $x_2 = x_1 + \delta_{v_x}$ and $y_2 = \frac{x_1 \cdot y_1}{x_1+(1-f)\delta_{v_x}}$ reserved in the pool. In this transantion (denoted as T_{A_2}), the bit will receive

$$\delta^{out}_{a_x} = \frac{x_2(1-f)\delta_{a_y}}{y_0+(1-f)\delta_{a_y}} = \frac{(x_0+\delta^{in}_{a_x}+\delta_{v_x})(1-f)\delta_{a_y}}{\frac{(x_0+\delta^{in}_{a_x})(\frac{x_0 \cdot y_0}{x_0+\delta^{in}_{a_x}(1-f)})}{x_0+\delta^{in}_{a_x}+(1-f)\delta_{v_x}}+(1-f)\delta_{a_y}}$$

token X. Hence, the profits of the bot P_a comes to be

$$P_a = \delta^{out}_{a_x} - \delta^{in}_{a_x} - 2b,$$

where $b \geq 0$ is the fixed and known base fee of the token X.



(a) Illustration of an ordinary Uniswap transaction. **(b) Illustration of a sandwich attacked Uniswap transaction.**

Figure 1. Illustration of a sandwich attack. In the left figure, the trade executes without being attacked, while the right one illustrates a sandwich attack in the Uniswap transaction.

3.3.2 Adversary perspective

Derived from the general game mechanism and from the predatory bots' perspective, the goal is to find the optimal attack input $\delta_{a_x}^{in}$ that could maximize their attack profits $P_a = \delta_{a_x}^{out} - \delta_{a_x}^{in} - 2b$. According to Heimbach et al.'s (2022) model, the case could be divided in to two different cases with respect to the slippage tolerance s. First, considering $s = 1$, which means s is not set by the trader, the bot's optimal attack input should be

$$\delta_{a_x}^{o} = \frac{(\delta_{v_x}(1-f)^2 x_0 - (2-f)f x_0^2) + \sqrt{\delta_{v_x}^2 (1-f)^3 x_0 (x_0 - (1-f)^2 f(\delta_{v_x} + x_0))}}{((2-f)f x_0 - \delta_{v_x}(1-f)^2 f)}$$

However, in most cases, traders will specify the slippage tolerance *s*, further limiting the maximum input size of the bots attack. Then, when $0 < s < 1$, the bot's optimal attack input to maximize profits should be

$$\delta_{a_x}^{s} = \frac{\frac{\sqrt{n(x_0, f, \delta_{v_x}, s)}}{1-s} - \delta_{v_x}(1-f)^3 - (2-f)(1-f)x_0}{2(1-f)^2},$$

where

$$n(x_0, f, \delta_{v_x}, s) = (1-f)^2(1-s)(\delta_{v_x}^2 (1-f)^4 (1-s)) + 2\delta_{v_x}(1-f)^2(2-f(1-s))x_0 + (4-f(4-f(1-s)))x_0^2$$

Combining these two cases, the final optimal input of the predatory bot should be

$$\delta_{a_x}^{in} = min\{\delta_{a_x}^{o}, \delta_{a_x}^{s}\}$$

Heimbach et al (2022) further proved that the bot's profit could not exceed the victim's loss given the equations, even adapting the optimal attack input.

3.3.3 Trader perspective

As for the traders, the goal is to minimize their costs (i.e., loss in attack) by finding the optimal slippage tolerance. First of all, given that the upper bound of the bot's profit cannot the victim's loss, the trader's transaction will be unattackable if

$$s \cdot \delta_{v_y} \geq 2b,$$

where b here is the fixed base fee for token Y. Therefore, we could get that higher slippage tolerances and larger trade sizes would make transactions more attackable. And we have any

$$s \leq s_a = \frac{2b}{\delta_{v_y}}$$

would give existence to the sandwich attack.

Then, we have any

$$s \leq s_r = \frac{p(s,\delta_{v_x})}{1-p(s,\delta_{v_x})}\left(\frac{(l+m)b}{\delta_{v_y}} + E(s|\bar{s} > s)\right)$$

would give existence to the sandwich attack.

Then, if $s_r < s_a$, we set optimal $s = s_a - \epsilon$, where $\epsilon \to 0^+$, if $s_r \geq s_a$, $s = s_r$.

3.3.4 Revised Sandwich Game

In order to assess the robustness of our model and the validity of our statistical analysis, we will repeat simulations with the same initial conditions but different seeds of the random number generator and parameter setting and use real data to conduct a comparative study and select the optimal simulation.

3.4 Real and simulated marketplace results comparison

In order to estimate, compare and evaluate the parameter setting of the proposed agent-based model, we acquire the real data of all Uniswap V2 AAVE⇌ETH transactions recorded on Ethereum under certain blocks to find the optimal simulation that could explain the reality.

For data acquisition, Flashbots developed a tool, "MEV-inspect-py", to detect MEV transactions from the collected transaction data. We can use it to find miner payments, token transfers and

profits, swaps, and sandwich attacks. With these conditions and tools meV-inspect-py, we can do all transactions related to Uniswap V2 through a large number of transactions.

We can run this tool locally on Kubernetes. After setting up the environment with Docker and Kind, we can select a block to check and connect to the Postgres database to see the data checks found in that block. We will calculate the mean square error of our simulated price with the actual price to decide the optimal simulation that could best reflect the characteristics of the AAVE market.

4. Results

4.1 Agent-based model

We coded the entire sandwich game process in Python in three parts: 1) the general mechanism of the game, 2) optimal attack input finding from the predatory perspective, and 3) optimal slippage tolerance finding from the trader's perspective, and tables of input and output for each perspective will be given below:

# Sandwich Game		
Input	s	Sllipage tolerance
	f	Transaction fee, $0 \leq f < 1$
	b	Base fee per transaction
	x_0	Token X reserved in the liquidity pool at time t_0
	y_0	Token Y reserved in the liquidity pool at time t_0
	δ_{v_x}	Token X entering the mempool at time t_0
	$\delta_{a_x}^{in}$	Token X charged when predatory bot first executes a transaction T_{A_1}, $\delta_{a_x}^{in} > 0$
Output	P_a	Profits of predatory bot

Table 1. Input and output for the general sandwich game model

# Adversary Perspective (find the optimal attack input $\delta_{a_x}^{in}$ that maximizes profits)		
Input	s	Slippage tolerance
	f	Transaction fee, $0 \leq f < 1$
	b	Base fee per transaction
	x_0	Token X reserved in the liquidity pool at time t_0

	y_0	Token Y reserved in the liquidity pool at time t_0
	δ_{v_x}	Token X entering the mempool at the time t_0, $\delta_{v_x} > 0$
Output	$\delta_{a_x}^{in}$	Optimal attack input for the predatory bot

Table 2. Input and output for the adversary perspective model

# **Trader's Perspective** (find the optimal slippage tolerance s that minimizes the costs)		
Input	f	Transaction fee, $0 \leq f < 1$
	b	Base fee per transaction
	x_0	Token X reserved in the liquidity pool at time t_0
	y_0	Token Y reserved in the liquidity pool at time t_0
	δ_{v_x}	Token X entering the mempool at time t_0
Output	s	Optimal slippage tolerance for the trader

Table 3. Input and output for the trader's perspective model

Specifically, the algorithm for the traders to get the optimal slippage tolerance is presented below as Algorithm 1:

Algorithm 1:

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 $s = s_r$

4.2 Data analysis

We analyze the effect of slippage tolerance (s), the transaction fee (f), and transaction size in relation to pool size (δ_{v_x}/x_0) on a predatory trading bot's maximal profit for a trader's trade.

We set the base fee to be 0, which removes the constant amount ($2b$) from the profit, and x_0 to 5000000 X. In Figure 2a, we set the (δ_{v_x}/x_0) to be 0.01, and in Figure 2b, we set the f to be 0.03.

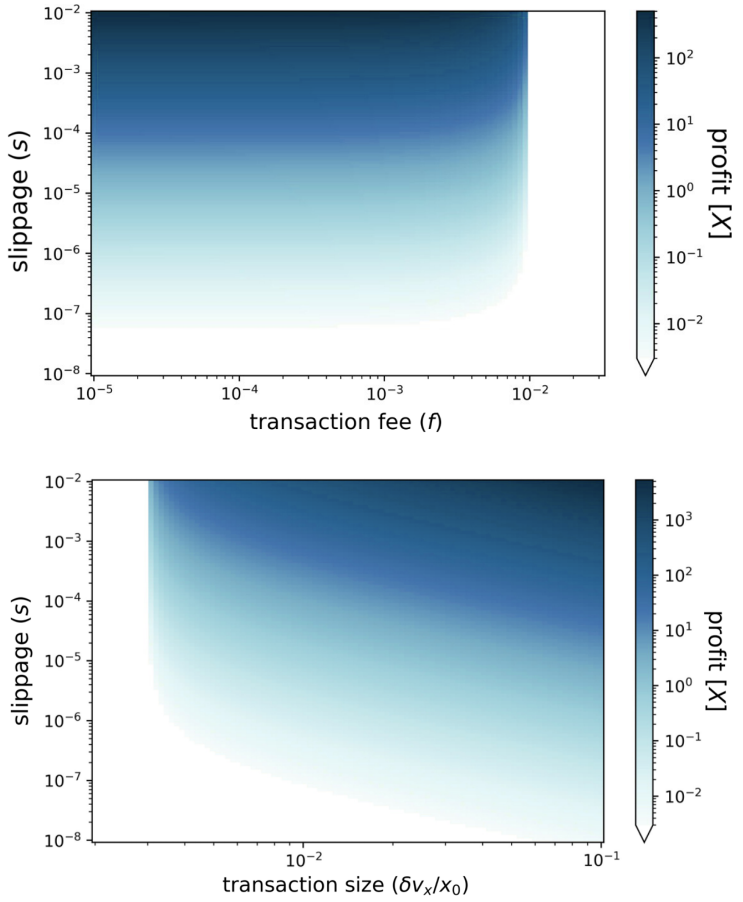


Figure 2. The effect of slippage tolerance (s), the transaction fee (f), and transaction size about pool size (δ_{v_x}/x_0) on a predatory trading bot's maximal profit

Figure 2a shows that the maximum profit of the robot depends on the slip tolerance and the transaction size. Even transactions with high slippage tolerance for small transaction sizes are unattackable. In addition, higher transaction fees allow for a high slippage tolerance before a trade becomes attackable.

4.3 Simulation results

By retuning the algorithm proposed by Heimbach et al. (2022), rational traders could protect themselves from sandwich attacks. Their consumption was reduced by automatic sliding better than Uniswap's recommendation in all tests settings. However, given the factoring theory, we hypothesized that behavioral and random traders are more vulnerable to sandwich attacks than

rational traders. However, this is unavoidable as some more conservative traders may prefer to accept the transaction order tax rather than accept the small risk that the transaction will fail. 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.

5. Conclusion and Discussion

5.1 Conclusion

Sandwich attacks remain a constant threat to traders trading on AMM. In this study, we extend the sandwich attack problem to include multiple types of traders and robots. Our model shows that rational traders defined under the optimal model can easily avoid most sandwich attacks by adjusting their slip tolerance and do not face an unnecessarily high risk of trade failure because their slip tolerance is not small enough. By retuning the algorithm proposed by Heimbach et al. (2022), rational traders could protect themselves from sandwich attacks, and their consumption was reduced by automatic sliding better than Uniswap's recommendation in all tests settings. However, given the factoring theory, we hypothesized that behavioral and random traders are more vulnerable to sandwich attacks than rational traders. This is unavoidable, however, as some more conservative traders may prefer to accept the transaction order tax rather than accept the small risk that the transaction will fail. 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.

5.2 Intellectual Merits

This study produces

1. The classification and definition of different traders based on the bounded theory in the DeFi Token trading market, including the theoretical basis of their different characteristics, the establishment of relevant assumptions, and quantitative formulas.
2. An agent-based model for the Uniswap AMM can simulate the sandwich attack.
3. Factors not taken into account by the model derived from the established model, which could serve as the practical foundation of an advanced multi-agent reinforcement learning model.

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 the 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.

5.3 Practical Impacts

Our study would greatly contribute to studying decentralized trading behavior and its impact on network evolution and economic performance. The proposed agent-based model has great potential to be extended from Aave to other DeFi products to the broader cryptocurrency market. 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.

5.4 Future Study

Considering the limitations and uncertainties in transaction data crawling on Uniswap, most of our model simulations currently adopt the mode of using dummy numbers and variable settings, and we will follow up with AMA Heimbach and Wattenhofer (2022) to ask them for further advice on data acquisition and some initial variable value calculation methods to make our model simulations more accurate and practical.

References

[Mybib Folder: ZiqiaoAo-SW-Report][https://www.mybib.com/j/InexpensiveDidacticRail]

"Aave/Aave-Protocol." n.d. GitHub. https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.

Angeris, Guillermo, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, and Tarun Chitra. 2020. "An Analysis of Uniswap Markets." *Cryptoeconomic Systems*, November. https://doi.org/10.21428/58320208.c9738e64.

Bovet, Alexandre, Carlo Campajola, Francesco Mottes, Valerio Restocchi, Nicolò Vallarano, Tiziano Squartini, and Claudio J. Tessone. 2019. "The Evolving Liaisons between the Transaction Networks of Bitcoin and Its Price Dynamics." *ArXiv:1907.03577 [Physics, Q-Fin]*, July. https://arxiv.org/abs/1907.03577.

Clippel, Geoffroy, and Kareen Rozen. 2021. "Bounded Rationality and Limited Data Sets." *Theoretical Economics* 16 (2): 359–80. https://doi.org/10.3982/te4070.

Cocco, Luisanna, Giulio Concas, and Michele Marchesi. 2015. "Using an Artificial Financial Market for Studying a Cryptocurrency Market." *Journal of Economic Interaction and Coordination* 12 (2): 345–65. https://doi.org/10.1007/s11403-015-0168-2.

Cocco, Luisanna, Roberto Tonelli, and Michele Marchesi. 2019. "An Agent-Based Artificial Market Model for Studying the Bitcoin Trading." *IEEE Access* 7: 42908–20. https://doi.org/10.1109/access.2019.2907880.

Fritsch, Robin, and Eth Zürich. 2021. “Concentrated Liquidity in Automated Market Makers.” https://arxiv.org/pdf/2110.01368.pdf.

Hanson, Robin. 2003. “Combinatorial Information Market Design.” *Information Systems Frontiers* 5 (1): 107–19. https://doi.org/10.1023/a:1022058209073.

Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro. 2021. “DeFi and the Future of Finance.” Papers.ssrn.com. Rochester, NY. April 5, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711777.

Heimbach, Lioba, and Roger Wattenhofer. 2022. “Eliminating Sandwich Attacks with the Help of Game Theory.” *ArXiv:2202.03762 [Cs]*, February. https://arxiv.org/abs/2202.03762.

Holmberg, Ulf, Tomas Sjögren, and Jörgen Hellström. 2012. “Comparing Centralized and Decentralized Banking: A Study of the Risk-Return Profiles of Banks.” Ideas.repec.org. February 17, 2012. https://ideas.repec.org/p/hhs/umnees/0838.html.

“Introduction to Aave - FAQ.” 2021. Aave.com. 2021. https://docs.aave.com/faq/.

Iori, G., and J. Porter. 2012. “Agent-Based Modelling for Financial Markets.” Www.city.ac.uk. 2012. https://openaccess.city.ac.uk/id/eprint/1744/.

Koens, Tommy, Pol Van Aubel, and Erik Poll. 2020. “Blockchain Adoption Drivers: The Rationality of Irrational Choices.” *Concurrency and Computation: Practice and Experience* 33 (8). https://doi.org/10.1002/cpe.5843.

LeBaron, Blake. 2000. “Agent-Based Computational Finance: Suggested Readings and Early Research.” *Journal of Economic Dynamics and Control* 24 (5): 679–702. https://doi.org/10.1016/S0165-1889(99)00022-6.

LeBaron, Blake, W.Brian Arthur, and Richard Palmer. 1999. “Time Series Properties of an Artificial Stock Market.” *Journal of Economic Dynamics and Control* 23 (9-10): 1487–1516. https://doi.org/10.1016/s0165-1889(98)00081-5.

Lehar, Alfred, and Christine Parlour. 2021. “Decentralized Exchanges.” https://www.snb.ch/n/mmr/reference/sem_2021_05_20_lehar/source/sem_2021_05_20_lehar.n.pdf.

Liu, Xiao-Yang, Hongyang Yang, Qian Chen, Runjia Zhang, Liuqing Yang, Bowen Xiao, and Christina Dan Wang. 2020. “FinRL: A Deep Reinforcement Learning Library for Automated Stock Trading in Quantitative Finance.” *ArXiv:2011.09607 [Cs, Q-Fin]*, November. https://arxiv.org/abs/2011.09607.

Lussange, Johann, Ivan Lazarevich, Sacha Bourgeois-Gironde, Stefano Palminteri, and Boris Gutkin. 2021. “Modelling Stock Markets by Multi-Agent Reinforcement Learning.” *Computational Economics* 57 (1): 113–47. https://doi.org/10.1007/s10614-020-10038-w.

Motamed, Amir Pasha, and Behnam Bahrak. 2019. “Quantitative Analysis of Cryptocurrencies Transaction Graph.” *Applied Network Science* 4 (1). https://doi.org/10.1007/s41109-019-0249-6.

Quick Note. 2021. “How to Make a Flash Loan Using Aave Explained - Step-By-Step Beginners Guides | QuickNode.” Www.quicknode.com. December 2021. https://www.quicknode.com/guides/defi/how-to-make-a-flash-loan-using-aave.

Schmitt, Noemi, Ivonne Schwartz, and Frank Westerhoff. 2020. “Heterogeneous Speculators and Stock Market Dynamics: A Simple Agent-Based Computational Model.” *The European Journal of Finance*, October, 1–20. https://doi.org/10.1080/1351847x.2020.1832553.

Simon, Herbert A. 1990. “Bounded Rationality.” *Utility and Probability*, 15–18. https://doi.org/10.1007/978-1-349-20568-4_5.

Vallarano, Nicoló, Claudio J. Tessone, and Tiziano Squartini. 2020. “Bitcoin Transaction Networks: An Overview of Recent Results.” *Frontiers in Physics* 8 (December). https://doi.org/10.3389/fphy.2020.00286.

Werner, Sam M., Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. 2021. “SoK: Decentralized Finance (DeFi).” NASA ADS. January 1, 2021. https://ui.adsabs.harvard.edu/abs/2021arXiv210108778W/abstract.

Whitepaper.io. 2020. “Aave Whitepaper - Whitepaper.io.” Whitepaper.io. January 2020. https://whitepaper.io/document/533/aave-whitepaper.

Part II: Supplementary Resources

1. Experts for Comments

Jakša Cvitanić: https://jaksacvitanic.com/

He is proficient in financial mathematics and also has research related to blockchain and cryptocurrency. I believe he can provide more professional advice on mathematics for our model.

2. Resources for Further studies

Financial Technology (FinTech) Innovations (University of Michigan)

This specialization is intended to familiarize learners with a broad range of financial technologies. While finance has always been at the forefront of technological innovation, the financial industry is changing rapidly in the face of new technology. In the past, at the forefront of innovation in finance were central governments and financial institutions. Today, information technology firms and professionals are leading innovation in the financial industry.

The goal is to show learners the genesis and use cases of the technology. Through this course, I can familiarize myself sufficiently with the technology that they can utilize and adapt the technologies in the future industry, thus finding the best application scenario for our study.

3. Seminar, Symposium, and Conference

- **MIT Sloan FinTech Conference 2022**

Part III: Related Products

1. Experiential Learning Activities

Independent Study in 22 Fall Semester Sessions 1&2

Are decentralized finance really decentralized? A social network analysis of AAVE protocol on Ethereum Blockchain

Ziqiao Ao, Gergely Horvath, Luyao Zhang

Abstract

Decentralized finance (DeFi) has the potential to disrupt centralized finance by validating peer-to-peer transactions through tamper-proof smart contracts and thus significantly lower the transaction cost charged by financial intermediaries. However, the actual realization of peer-to-peer transactions and the levels and effect of decentralization is mainly unknown. Our research applies social network analysis to measure the level, dynamics, and impacts of decentralization in DeFi token transactions on the Ethereum blockchain. First, we find a significant core-periphery structure in the AAVE token transaction network where the cores include the two largest centralized crypto exchanges. Second, we evidence that multiple networks features consistently characterize decentralization dynamics. Finally, we document that a more decentralized network significantly predicts a higher return and lower volatilities of the DeFi tokens. We point out that our approach is seminal in inspiring future extensions in the facets of application scenarios, research questions, and methodologies.

Keywords: Decentralized Finance, Social Network Analysis, AAVE, Ethereum, core-periphery, modularity, giant component ratio

Link to the manuscript (not published yet)

2. Seminar, Symposium, and Conference Presentations

Guest Speaker on Intelligent Economy Lecture

ECON 211-001 (1094) Intelligent Economics: An Explainable AI Approach

2021 Autumn Term (Seven Week – Second Session)

Instructor: Luyao (Sunshine) Zhang | Ph.D. in Economics

Ziqiao Ao (Coordinator: Jingwei Li):

Time: Nov 9, 9:00 PM China Time;

Format: Online

Intro: I was invited as a guest speaker in Prof. Luyao Zhang's ECON211 class to present my independent study on the DeFi network, supervised by Prof. Luyao Zhang and Prof. Gergely Horvath, and produce the presentation video together with the Q&A documents.

Presentation Slides: **DeFi Network Study**

3. Publications

First Co-author Conference Paper

Deep Learning Ethereum Token Price Prediction on Dynamic Network and Time Series Analysis

Ziqiao Ao [1]*, Jiayi Li [1], Haoxin Yu [1]
Nature Science Department
Duke Kunshan University

***Abstract*—**Ethereum has recently surged in popularity, as it can hold various digital tokens and decentralized applications. This paper aims to predict UNI's price in USD through dynamic network analysis and time-series analysis. Previous research in this field rarely considers comprehensive network analysis while predicting token price. This paper puts forward a

strengthened Bidirectional LSTM model that includes token economical features and network features. We use Root Mean Squared Error (RMSE) to verify the validity and compare it with other LSTM and GRU models on performance. Lastly, a logarithm difference method for data preprocessing was introduced to resolve the lag problems.

Keywords - *Blockchain; Ethereum ERC20; Network Analysis; Deep Learning; Price Prediction*

**Link to the paper (not public yet)*

Accepted by **2021 International Conference on Data Mining and Statistical Applications (DMSA)**, and will be published by **IEEE Xplore** in June.

Intro to Conference

DMSA 2021, held in Chengdu on Oct 29-31, 2021, focuses on the latest research fields of "Data Mining and Statistical Applications", providing an international platform for experts, professors, scholars, engineers, and others from universities, scientific institutes, enterprises, and public institutions at home and abroad to share professional experience, expand the professional network, communicate new ideas face to face and display research results. Exploring key challenges and research directions in this field, with a view to promoting the development and application of theories and technologies in this field in universities and enterprises, as well as establishing business or research connections for attendees and seeking global partners for future ventures.

4. Fellowship, Grants, Offers

Is Ethereum Decentralized? An interdisciplinary study of social network studies, agent-based modeling, and game theory in distributed systems.

Ziqiao Ao, Gergely Horvath, Luyao Zhang

**Link to the proposal (not public yet)*

Proposal applied for **the Ethereum Foundation academic research grant**

Part IV: Signature Work Documents

Document type	URL to PDF
SW Declaration of Intent	https://drive.google.com/file/d/12tn8ZZTvs0owD_K1NC29rxmLfjXF_XiA/view?usp=sharing
SW Mentor Agreement Form	https://drive.google.com/file/d/1hskWJ7ZTW2o84cJXlfrSRy-t1y952Gl_/view?usp=sharing
Team-Based Project Agreement Form	https://drive.google.com/file/d/1-RB0fxHeSINNxoQvrPjhhe_nrQwUu4en/view?usp=sharing
SW Project Proposal Form	https://drive.google.com/file/d/103um6dA6wN2z7dTBbFo2qdrFyvyL2Y03/view?usp=sharing
SW Experiential Learning Proposal Form	
SW Experiential Learning Report Form	https://drive.google.com/drive/u/0/folders/1p1SpWc6qd-mA55zQe3w2JVf7gemeTTlC
SW Experiential Learning Supervisor Report Form	https://drive.google.com/drive/u/0/folders/1p1SpWc6qd-mA55zQe3w2JVf7gemeTTlC
RCR Certificate	https://drive.google.com/file/d/1zp1A9bYaO_7ZgDiDz5A-EGHZjy5fiilq/view?usp=sharing
Petition to Change SW Project Proposal Form	https://drive.google.com/drive/u/0/folders/1p1SpWc6qd-mA55zQe3w2JVf7gemeTTlC
SW Poster	https://drive.google.com/drive/u/0/folders/1p1

	SpWc6qd-mA55zQe3w2JVf7gemeTTlC
SW Presentation Video	https://drive.google.com/drive/u/0/folders/1p1SpWc6qd-mA55zQe3w2JVf7gemeTTlC