

Cyclic Arbitrage in Decentralized Exchanges

Ye Wang
wangye@ethz.ch
ETH Zurich
Zurich, Switzerland

Yan Chen
bitmaster@zju.edu.cn
Zhejiang University
Hangzhou, China

Haotian Wu
wu558536@stu.xjtu.edu.cn
Xi'an Jiaotong University
Xi'an, China

Liyi Zhou
liyi.zhou@imperial.ac.uk
Imperial College London
London, United Kingdom

Shuiguang Deng
dengsg@zju.edu.cn
Zhejiang University
Hangzhou, China

Roger Wattenhofer
wattenhofer@ethz.ch
ETH Zurich
Zurich, Switzerland

ABSTRACT

Decentralized Exchanges (DEXes) enable users to create markets for exchanging any pair of cryptocurrencies. The direct exchange rate of two tokens may not match the cross-exchange rate in the market, and such price discrepancies open up arbitrage possibilities with trading through different cryptocurrencies cyclically. In this paper, we conduct a systematic investigation on cyclic arbitrages in DEXes. We propose a theoretical framework for studying cyclic arbitrage. With our framework, we analyze the profitability conditions and optimal trading strategies of cyclic transactions. We further examine exploitable arbitrage opportunities and the market size of cyclic arbitrages with transaction-level data of Uniswap V2. We find that traders have executed 292,606 cyclic arbitrages over eleven months and exploited more than 138 million USD in revenue. However, the revenue of the most profitable unexploited opportunity is persistently higher than 1 ETH (4,000 USD), which indicates that DEX markets may not be efficient enough. By analyzing how traders implement cyclic arbitrages, we find that traders can utilize smart contracts to issue atomic transactions and the atomic implementations could mitigate users' financial loss in cyclic arbitrage from the price impact.

CCS CONCEPTS

• General and reference → Empirical studies; Measurement; • Applied computing → Economics.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

Conference'17, July 2017, Washington, DC, USA

© 2022 Association for Computing Machinery.

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00

<https://doi.org/10.1145/nnnnnnn.nnnnnnn>

KEYWORDS

Blockchain, Ethereum, Decentralized Exchanges (DEXes), Cyclic Arbitrage

ACM Reference Format:

Ye Wang, Yan Chen, Haotian Wu, Liyi Zhou, Shuiguang Deng, and Roger Wattenhofer. 2022. Cyclic Arbitrage in Decentralized Exchanges. In *Proceedings of ACM Conference (Conference'17)*. ACM, New York, NY, USA, 12 pages. <https://doi.org/10.1145/nnnnnnn.nnnnnnn>

1 INTRODUCTION

Decentralized finance (DeFi) in the blockchain ecosystem has attracted a surge of interest with a total gross value locked (GVL) of up to 120 billion USD by October 2021 [3]. DeFi applications are smart contracts deployed on blockchains, which support a wide variety of financial services [29, 38]. One of the important applications is decentralized exchange (DEX). DEXes allow users to exchange their crypto-assets and ensure decentralized and non-custodial trading. Traders sell and buy assets on DEXes by interacting with smart contracts on the blockchain with no centralized authority being involved. In an automated market maker (AMM) DEX, the exchange rate of each trade is determined by predefined algorithms and market liquidity reserves. Most prominent DEXes in the blockchain ecosystem are AMM DEXes, such as Uniswap [7] and SushiSwap [4].

The exchange rates between different pairs of cryptocurrencies (also known as tokens) in AMM DEXes are not always in sync perfectly, which opens up arbitrage possibilities for cyclic trading. Assume we have three tokens A, B, C , and three markets between any two tokens: $A \rightleftharpoons B, B \rightleftharpoons C$ and $C \rightleftharpoons A$. Traders are able to trade tokens cyclically: Traders can exchange A for B in $A \rightleftharpoons B$, then B for C in $B \rightleftharpoons C$, and finally C for A in $C \rightleftharpoons A$ again, to benefit themselves from the price discrepancies. The combination of these three trades of tokens is a cyclic arbitrage (transaction).¹ Figure 1

¹The particular case with three tokens is called triangular arbitrage [19, 33].

shows an example of cyclic arbitrage happened on October 30, 2020.

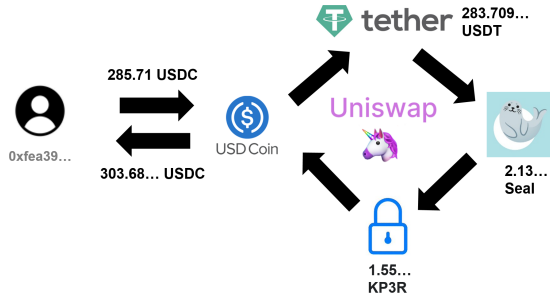


Figure 1: An example cyclic arbitrage on Uniswap V2: The trader traded 285.71 USDC through four different exchange markets across USDC, USDT, Seal, Kp3r, and finally received 303.68 USDC. The revenue of this cyclic arbitrage is 17.97 USDC (18 USD).

In this paper, we provide a systematical study on cyclic arbitrage, with (a) theoretical analysis and (b) empirical evaluation with transaction-level data. We first propose a theoretical framework for studying cyclic arbitrage in AMM. Then, we use the theoretical model to analyze the profitability conditions and optimal trading strategies of cyclic arbitrage in the most common AMM, the constant product market maker (CPMM). We further utilize our theoretical results to investigate market data. We examine exploitable arbitrage opportunities on Uniswap V2 [7] from May 4, 2020, to April 15, 2021. We find that in almost every block, the revenue of the most exploitable arbitrage opportunity is higher than 1 ETH (4,000 USD). The total revenue of exploitable arbitrage opportunities is persistently higher than 10 ETH over four months, which suggests that the market efficiency of DEXes might be limited. Later, we measure the market size of exploited cyclic arbitrage in Uniswap V2. We observe 292,606 cyclic transactions over eleven months. Traders receive a total revenue beyond 34,429.11 ETH and pay 8,458 ETH as gas fees. The market size of exploited cyclic arbitrage is significantly smaller than the exploitable opportunities because of the wide variety of tokens and the high gas fees. Finally, we investigate the implementations of cyclic arbitrage. We find that only 0.03% of traders submit trades sequentially with multiple blockchain transactions for a single cyclic arbitrage. Alternatively, traders always utilize smart contract technology to submit a cyclic arbitrage within a single blockchain transaction. Such atomic implementations mitigate the financial loss of users in cyclic arbitrage.

To the best of our knowledge, this is the first paper to study the traders' arbitrage behavior of cryptocurrency theoretically and empirically. We make the following contributions. First, we provide a systematical understanding of

cyclic arbitrage, with the theoretical analysis of the arbitrage model, the measurement of exploitable arbitrage opportunities, the measurement of exploited cyclic arbitrage, and the measurement of cyclic arbitrage implementations. Second, we provide the measurement of state-of-the-art in terms of (cyclic) arbitrages in DEXes. Finally, we reveal that blockchain technology enables users to explore more trading strategies. Further studies in DEXes may provide us with novel understandings of user behaviors in financial markets.

2 BACKGROUND AND RELATED WORK

2.1 Ethereum and Smart Contract

Ethereum is a public blockchain platform, which supports Turing complete functions [44]. In contrast to earlier blockchain systems such as Bitcoin, Ethereum allows for decentralized peer-to-peer transactions, and has generic computation capabilities through smart contracts. A smart contract is a set of programs written in high-level languages, e.g., Solidity. Creators compile these programs into executable byte-code and deploy the smart contract on Ethereum.

There are two kinds of accounts in Ethereum: (a) externally owned accounts (EOAs), i.e., those controlled by human users with the corresponding private key, and (b) smart contract accounts (CAs), i.e., those controlled by executable code [44]. An Ethereum transaction is broadcast by an EOA to the Ethereum network, while miners then collect transactions and record them in blocks. EOAs can send three types of transactions: *simple transaction*, to transfer the native currency, ETH; *smart contract creation transaction*, to create a new smart contract; and *smart contract execution transaction*, to execute a specific function of a smart contract.

When a transaction is included in blocks by miners, the operation corresponding to the message takes effect. The miner who creates the block modifies the state of corresponding accounts. Each step of the miner's operation consumes a certain amount of gas, and the amount of gas consumed in each block is capped. Users need to specify a gas price for the operation execution when sending transactions. The fee paid by the initiator of transactions to miners is determined by the amount of gas consumed and the gas price (gas fee = gas price \times gas consumption). The miner records receipts of the executed transactions in Ethereum blocks, including the information of the gas fee, the identity of the transaction, and other information generated by smart contracts during the execution.

2.2 Decentralized Exchanges (DEXes)

Based on the support of the smart contract, users can create cryptocurrencies on Ethereum in addition to the native coin ETH [12]. As of October, 2021, more than 450,000 tokens exist on Ethereum platform [5]. Such development of the

blockchain ecosystem incentivizes the emergence of on-chain financial systems, i.e., Decentralized Finance (DeFi). DeFi applications are smart contracts deployed on Ethereum, which support sophisticated financial services, such as borrowing and lending [27], asset exchanges [7], leverage trading [1], as well as novel applications such as flash loans [40].

Decentralized exchanges (DEXes) are one of the financial infrastructures of the blockchain ecosystem. Compared to centralized exchanges (CEXes), DEXes do not involve any centralized operators. Users do not need to transfer their assets to the operator before conducting market operations [22]. In contrast, they send on-chain transactions to DEXes smart contracts to place orders while they keep control of their assets during the entire process. DEXes support mutual trades among different cryptocurrencies. The prevalent DEX mechanisms operate through so-called automated market makers (AMM), which aggregate liquidity (i.e., cryptocurrencies) within liquidity pools contributed by liquidity providers. Traders can exchange cryptocurrencies with the liquidity pool and pay commission fees to the liquidity providers. For example, when traders want to exchange cryptocurrency A for B , they can call a smart contract function that transfers A from the traders' accounts to the liquidity pool between A and B . The liquidity pool then sends B to the traders' account. The exchange process does not involve the participation of any other traders. The exchange rate between A and B is determined by transparently predefined functions encoded in the DEX smart contract.

The constant product function is one of the most widely used pricing mechanism. Assume a trader want to exchange δ_a of A for B token and the liquidity of A and B are a and b , respectively. The following equation always hold during the transaction: $a \cdot b = (a + \delta_a \cdot r_1) \cdot (b - \frac{\delta_b}{r_2})$, where r_1 and r_2 denote the commission fee in asset A and B respectively. In Uniswap [7], $r_1 = 0.997$ and $r_2 = 1$, which indicates that the commission fee is equal to $0.3\% \cdot \delta_a$. The remaining liquidity in the pool equals to $(a + \delta_a, b - \frac{r_1 \cdot r_2 \cdot b \cdot \delta_a}{a + r_1 \cdot \delta_a})$.

2.3 Arbitrage in Cryptocurrency Markets

Research on arbitrage in cryptocurrencies is still in its beginning. Previous studies focus on either theoretical analysis of the behavior of miners and traders in blockchain systems [9, 16, 17, 24–26, 30, 32, 35, 41, 42], or the influence of cryptocurrencies as a potential payment and transaction mechanism in financial markets [8, 11, 15, 21, 23, 36].

Some recent studies [10, 20, 31, 34, 37] have noted the prices discrepancies of cryptocurrencies in CEXes. Makarov and Schoar [31] studied price deviations and potential arbitrage opportunities of Bitcoin, Ethereum, and Ripple for 34 CEXes across 19 countries. They observed significant

market segmentation among different countries and suggested that capital controls are the main reasons for market segmentation. Nan and Kaizoji [34] studied the potential triangular arbitrage with Bitcoin, Euro and U.S. dollar and analyzed market data with a bivariate GARCH model. Nevertheless, previous studies have only investigated exploitable arbitrage opportunities in CEXes, and none of them have measured exploited arbitrages in the market. Meanwhile, the arbitrage strategy they studied has many constraints to be implemented in markets, such as cross-border capital controls and instantaneous transfers between CEXes.

Recently, DEXes have attracted attention worldwide as an emerging alternative of CEXes for exchanging cryptocurrencies. Daian et al. [13, 14] have analyzed the fundamental weakness of DEXes: slow (on-chain) trading. Since transactions are broadcast in the Ethereum network, adversaries can observe profitable transactions before they are executed and place their own orders with higher fees to front-run the target victim. Front-running attackers bring threats to the market and system stability. Arbitrageurs optimize network latency aggressively and conduct priority gas auctions to front-run profitable trades [28], which results in excessive transaction fees affecting normal users in blockchain ecosystems. Moreover, because of the high miner-extractable value, fee-based forking attacks and time-bandit attacks are created and bring systemic consensus-layer vulnerabilities. Zhou et al. [45] and Torres et al. [18] studied sandwiching attacks, i.e., combinations of front and back-running, in DEXes. When observing a victim transaction, attackers place one order just before it (front-run) and place an order just after it (back-run) to benefit themselves through the variance of the exchange rates. Qin et al. [39] quantified the revenue of arbitrages in DEXes. However, this work lacks a systematic analysis of arbitrage behavior and only measures the exploited arbitrage opportunities of 144 cryptocurrencies.

Compared to previous studies, our work fills the following two research gaps to provide a more comprehensive understanding of cyclic arbitrage. First, we do not only consider potential arbitrage opportunities in the market but also compare with exploited arbitrage opportunities. Second, we examine different implementations of arbitrage strategies in DEXes and discuss how smart contract technology could help traders to mitigate the financial loss from the price impact.

3 CYCLIC ARBITRAGE MODEL

In this section, we propose a theoretical framework of cyclic arbitrage, and then examine the profitability and the optimal revenue of cyclic arbitrage in CPMM.

Arbitrage model: A cyclic transaction between n tokens A_1, A_2, \dots, A_n is a sequence of n trades:

Trade 1: Exchange δ_1 of A_1 with δ_2 of A_2 .

Trade 2: Exchange δ_2 of A_2 with δ_3 of A_3 .

...

Trade n: Exchange δ_n of A_n with δ'_1 of A_1 .

Note that the output of *Trade i* exactly equals to the input of *Trade i + 1*, while the revenue of the cyclic transaction is differences between the output of *Trade n* and the input of *Trade 1*, i.e., $\delta'_1 - \delta_1$.

As we state in the introduction, the exchange rates between different token pairs may not be synchronized perfectly. However, it is not clear under which conditions that exploitable arbitrage opportunities exist in the market as users also need to pay the commission fee for each trade. Therefore, we analyze the profitability and the optimal trading strategy of a cyclic arbitrage in CPMM.

Profitability conditions: Assume we have three tokens A_1, A_2 , and A_3 , and three liquidity pools between three tokens. We denote $a_{i,j}$ as the amount of reserved A_i in the liquidity pool with token A_j . Then, the revenue of trading δ_1 of token A_1 through the cycle $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow A_1$ is

$$\delta'_1 - \delta_1 = \left(\frac{r_1 \cdot r_2 \cdot \frac{r_1^2 \cdot r_2^2 \cdot a_{2,1} \cdot a_{3,2} \cdot a_{1,3}}{a_{2,3} \cdot a_{3,1} + r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,1} + r_1^2 \cdot r_2^2 \cdot a_{2,1} \cdot a_{3,2}}}{\frac{a_{1,2} \cdot a_{2,3} \cdot a_{3,1}}{a_{2,3} \cdot a_{3,1} + r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,1} + r_1^2 \cdot r_2^2 \cdot a_{2,1} \cdot a_{3,2}} + r_1 \cdot \delta_1} - 1 \right) \cdot \delta_1.$$

Traders can benefit from the cyclic transaction only if the revenue, i.e., $\delta'_1 - \delta_1$, is larger than 0. We generalize the profitability conditions for n tokens in Theorem 1. In general words, only if the arbitrage index, i.e., the product of n exchange rates along the cycle, is larger than the commission fees paid in the n pools, there exists exploitable cyclic arbitrage opportunity.

THEOREM 1 (CF. APPENDIX A). *For a given cycle $A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n \rightarrow A_1$ with n tokens, there exists an arbitrage opportunity for the cyclic transaction if the product of exchange rates $\frac{a_{2,1} \cdot a_{3,2} \cdot \dots \cdot a_{n,1}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,1}} > \frac{1}{r_1^n \cdot r_2^n}$, where $a_{i,j}$ denotes the liquidity of token A_i in the liquidity pool with token A_j . Meanwhile, the arbitrage cannot benefit from the reversed direction $A_1 \rightarrow A_n \rightarrow \dots \rightarrow A_2 \rightarrow A_1$ for cyclic transactions.*

Optimal trading strategy: In addition to noticing whether there are exploitable cyclic arbitrage opportunities in markets with Theorem 1, it is also important for traders to find a proper trading strategy to maximize the revenue. It is intuitive that if the derivative of the revenue function to the initial trading amount is zero, then we acquire the optimal revenue. We design an algorithm to compute the optimal trading volume of a cyclic arbitrage (cf. Algorithm 1). If we exchange δ_1 of A_1 through the cycle to obtain δ_n of A_n , we can equate this behavior as exchanging δ_1 of A_1 in another liquidity pool between A_1 and A_n where the amount of reserved tokens of A_1 and A_n are $a'_{1,n}$ and $a'_{n,1}$ respectively. We then further compute the optimal trading volume for the cyclic transaction

Algorithm 1 Compute the equivalent liquidity of the cycle

```

1:  $a'_{1,n} \leftarrow a_{1,2}$ 
2:  $a'_{n,1} \leftarrow a_{2,1}$ 
3: for  $i$  from 2 to  $n - 1$  do
4:    $a'_{1,n} \leftarrow \frac{a'_{1,n} \cdot a_{i,i+1}}{a_{i,i+1} + r_1 \cdot r_2 \cdot a'_{n,1}}$ 
5:    $a'_{n,1} \leftarrow \frac{r_1 \cdot r_2 \cdot a'_{n,1} \cdot a_{i+1,i}}{a_{i,i+1} + r_1 \cdot r_2 \cdot a'_{n,1}}$ 
6: end for

```

through $A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n \rightarrow A_1$ as $\delta_a^{op} = \frac{\sqrt{r_1 \cdot r_2 \cdot a' \cdot a} - a}{r_1}$, where $a = \frac{a'_{1,n} \cdot a_{n,1}}{a_{n,1} + r_1 \cdot r_2 \cdot a'_{n,1}}$ and $a' = \frac{r_1 \cdot r_2 \cdot a_{1,n} \cdot a'_{n,1}}{a_{n,1} + r_1 \cdot r_2 \cdot a'_{n,1}}$. We refer readers to Appendix B for a detailed analysis.

4 CYCLIC ARBITRAGE OPPORTUNITIES

From Algorithm 1, we can infer that only the amounts of reserved tokens in liquidity pools and the trading direction are needed for determining the optimal trading strategies. When an Ethereum block is published, the updated information of liquidity pools is available to all traders. Therefore, with our theoretical model, we are able to investigate exploitable cyclic arbitrage opportunities in DEXes. We choose Uniswap V2 as the example for the empirical analysis because Uniswap V2 has the longest operation time, the most active traders, and the most liquidity pools among all DEXes [2, 6].

Data collection: Every market operation on Uniswap is recorded on Ethereum blocks. We launch go-ethereum, an Ethereum client, on our server to collect data from block 10000835 (when Uniswap V2 has been deployed, 4th May 2020) to block 12244144 (15th April 2021). We observe that a Sync event is recorded in the blockchain receipt when a market operation happens on Uniswap, and the event includes the liquidity of tokens in the pool after the market operation. Therefore, by collecting all Sync events, we are able to recover the market states of all liquidity pools on Uniswap V2 over time. More precisely, we build a dataset that includes the liquidity reserved in all liquidity pools on Uniswap V2 after the execution of transactions in each block.

Profitable opportunities: With such a dataset, we find profitable cycles in the market and compute the optimal trading input of each exploitable cyclic transaction and the corresponding revenue. We consider exploitable cyclic arbitrage opportunities within the cycles with length three that involve ETH. As more than 80% liquidity pools in Uniswap V2 are between ETH and another cryptocurrency [43], we infer that we provide a reasonable lower bound for estimating the exploitable opportunities.

Because most Ethereum transactions pay more than 0.0001 ETH as gas fee to miners, we count the number of cycles that

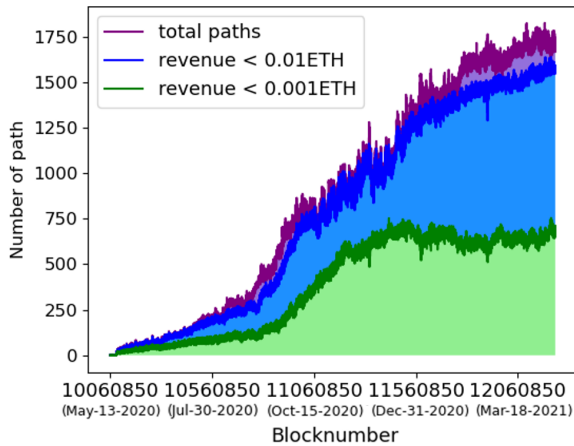


Figure 2: Number of exploitable opportunities in Uniswap V2 over time. The purple line represents the number of cycles that provide revenue higher than 0.0001 ETH. The green represents the number of cycles whose revenue is under 0.001 ETH. The blue line represents the number of cycles whose revenue is under 0.01 ETH.

can provide revenue higher than 0.0001 ETH in Figure 2.² The number of exploitable arbitrage opportunities has increased to 1,750 in eleven months. However, we should not overestimate the potential revenue as some cyclic strategies are mutually exclusive. For instance, if two cycles involve the same pair of tokens, only one of them can be exploited with the optimal trading volume.

Therefore, we consider a set of independent cycles (none of them involves the same liquidity pool) at each block and sum up the revenue of exploiting them, which provides a lower bound of the total revenue that traders can take from the market over time (cf. Figure 3). We find that since July 2020, when the market has been developing, the potential revenue of cyclic arbitrage in each block reaches 100 ETH, while the maximum revenue of a single cycle is higher than 10 ETH. However, between November 2020 and March 2021, the total potential revenue per block drops to less than 10 ETH.

Remarks: Previous studies on arbitrage opportunities of cryptocurrency have mainly focused on CEXes. Compared with their results, we find the following two characteristics of cyclic arbitrage opportunities in DEX.

Wider range of arbitrage: Since CEXes operators will audit the cryptocurrencies trading on the platform, and DEXes support any trading pairs of tokens, the range of the market is wider in DEXes, which further introduces arbitrage

²The basic gas consumption of a Uniswap transaction is higher than 100,000 and the gas price is always higher than 1 GWei (10^{-9} ETH per gas).

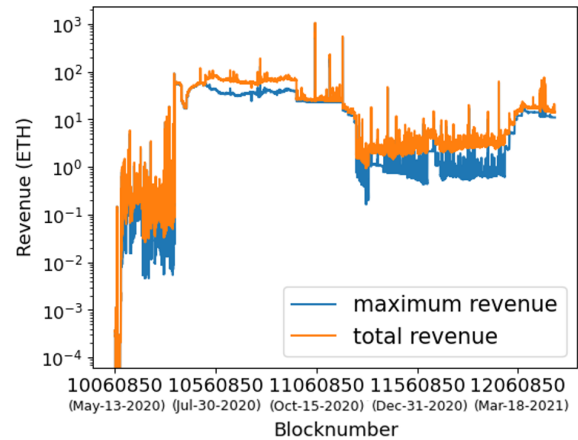


Figure 3: Exploitable revenue of cyclic arbitrage in each block. The blue line represents the maximum revenue of a single arbitrage opportunity, while the orange line represents the sum of a set of independent cyclic arbitrage opportunities.

opportunities across a broader range of cryptocurrencies. For instance, at the time of writing the paper, Uniswap V2 enables trades between 30,000 tokens while Binance, one of the biggest CEX, only supports less than 400 tokens. We find that more than 2890 liquidity pools and 1143 tokens have been involved in arbitrage opportunities larger than 0.1 ETH (400 USD), which indicates that the range of tokens in cyclic arbitrage is wider in DEXes than CEXes (1,143 vs. 400).

Larger market size: Compared to the arbitrage market in CEXes, the market size in DEXes are larger. As reported by Makarov and Schoar [31], the potential arbitrage revenue between 34 CEXes is 2 billion USD over four months (16 million USD per day). However, in a single DEX, i.e., Uniswap V2, as the exploitable revenue of each block exceeds 1 ETH and there are 6,000 blocks per day, the daily revenue is much higher than 24 million USD, even reaching 240 million USD. Moreover, the arbitrage index in CEXes is always lower than 1.1 [31]. However, the maximum revenue of a single arbitrage opportunity in Uniswap V2 is persistently larger than 1 ETH since July 2020, which suggests that it might be more efficient to exploit arbitrage opportunities in DEXes than in CEXes.

5 ARBITRAGE MARKETS

After noticing the exploitable arbitrage opportunities in Uniswap V2, we further investigate how many cyclic arbitrages have been executed in the market and how much revenue traders have exploited.

Data collection: For each successful exchange between two tokens, a *Swap* event will be recorded in the blockchain

sync / swap.

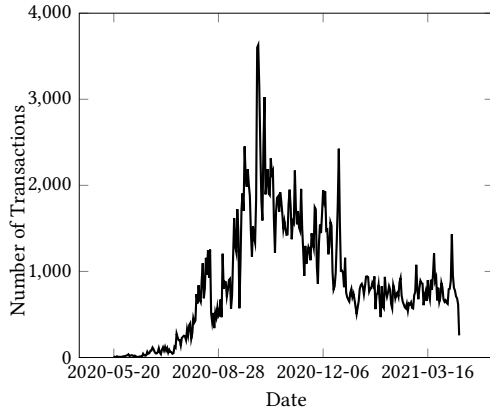


Figure 4: Daily number of cyclic arbitrages.

receipt, and the event includes all trading information, including the input amount of tokens and the output amount tokens. Therefore, we can use the heuristics in Section 3 to determine cyclic transactions. Note that apart from the heuristics mentioned before, we recognize a cyclic transaction such that all trades are executed within 100 blocks (25 minutes). Because of the volatility in the market price, it is hard to argue that two trades with a time gap of 25 minutes is for exploiting a cyclic arbitrage opportunity.

Overall statistics: Until April 15, 2021, we find 292,606 cyclic transactions, while 287,241 of them start with ETH. These arbitrages happened in 17,189 different cycles. The most popular cycle is ETH-LCX-REVV with 4710 arbitrages. Only 265 cycles have been exploited more than ten times. Around 85% of cyclic transactions (247,297) are implemented with cycle of length 3. These observations are consistent with our claims in Section 4 that the DEXes have a broad range of cryptocurrencies in arbitrage, and counting the cycle with length three can provide a reasonable lower bound of cyclic arbitrage opportunities.

Transaction number: Figure 4 shows the daily number of cyclic transactions in Uniswap. Traders started to perform cyclic arbitrage from May 20, 2020, two weeks after the start of Uniswap V2 (May 04, 2020). From May 2020 to September 2020, the market has been growing, reaching more than 3,000 cyclic transactions per day, and then the market enters a relatively active period with more than 1,000 cyclic transactions per day. The market becomes consistent and stable after January 2021, with 600 transactions per day.

Transaction revenue: Because more than 98% of cyclic transactions start with ETH and there might be error if we sum up the revenue of different cryptocurrencies, we report the revenue of those that start with ETH to provide a reasonable lower bound of the market size. Figure 5 shows the cyclic

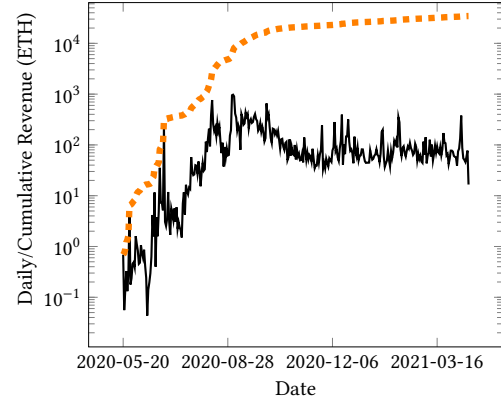


Figure 5: Revenue of cyclic transactions in Uniswap (in ETH). The black line shows a daily market size. The dotted orange line shows the cumulative market size.

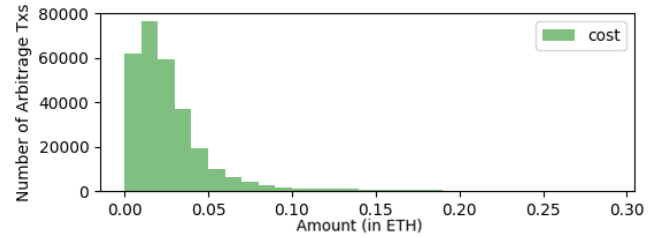


Figure 6: Distribution of gas fee per transaction.

arbitrage market size, denominated in ETH. The black line shows the daily revenue of cyclic transactions, and the dotted orange line shows the cumulative revenue of cyclic transactions. The total revenue of cyclic arbitrage with ETH in Uniswap V2 is 34,429 ETH. At the early stage of the market (from May to July 2020), the market of cyclic arbitrage is negligible, i.e., always less than 10 ETH per day. Later on, the daily arbitrage market has increased to 1000 ETH, while traders become strategic, and the average revenue per transaction increases to 0.2 ETH until September 2020. Since October 2020, the market has become relatively stable with 100 ETH revenue per day, and the average revenue of each cyclic transaction is around 0.1 ETH. After January 2021, although the daily number of cyclic arbitrage decreases, the total revenue keeps at the same level as before, which indicates that traders can exploit more profitable arbitrage opportunities.

Transaction cost: Apart from commission fees paid to liquidity providers that have been considered in our theoretical model, traders also need to pay gas fees to miners for executing their market operations. Figure 6 shows the distribution

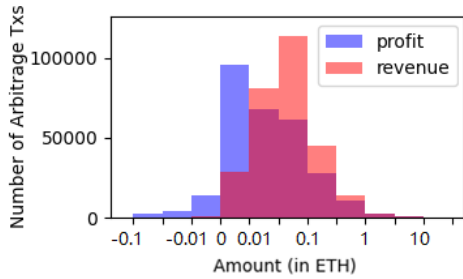


Figure 7: Distribution of profit and revenue per transaction.

of the gas fee of cyclic transactions. Around half of transactions (48%) cost less than 0.02 ETH as the gas fee. The total gas fee (8,458 ETH) accounts for 24.6% of the total revenue (34,429.11 ETH) of cyclic transactions. Figure 7 compares arbitrage income and net profit for cyclic arbitrages. Only 7.1% of cyclic arbitrages result in negative profits. Gas fees drive revenue per cyclic arbitrage from 0.01-0.3 ETH gross revenue to 0-0.1 ETH net profit, where the majority of cyclic arbitrages (78.4%) falling in this range.

Remarks: Compared to arbitrage opportunities in the market, we find that although exploitable arbitrage opportunities exist in almost every block, there are much fewer cyclic arbitrage transactions happening in the market, which might indicate that DEXes are not efficient enough. Since the DEXes are fully built on the blockchain systems, there is a limitation of trading volume on the market. Moreover, because of the large size of DEXes, it will take traders time to find cycles with revenue to cover gas fees, as the gas fee of half cyclic arbitrage exceeds 0.02 ETH.

6 ARBITRAGE IMPLEMENTATIONS

After studying exploited cyclic arbitrage opportunities, we continue to analyze how users implement their cyclic arbitrage strategies in the market. In this section, we study the implementations of cyclic arbitrage in DEXes from two perspectives. We first analyze how traders interact with smart contracts to mitigate the financial loss in cyclic arbitrage. Then, we examine the success rate in exploiting arbitrage opportunities of different methods.

Sequential implementation and atomic implementation: In traditional CEXes markets, after observing arbitrage opportunities, traders may directly submit n separate orders to realize the cyclic arbitrage. In DEXes, traders have different implementations with smart contract technology: sequential implementation and atomic implementation. Sequential implementation is similar to arbitrage implementations in CEXes. Traders submit n orders separately with n blockchain transactions, while these n transactions are executed sequentially.

On the other hand, traders can deploy smart contracts to group all the n trades of a cyclic arbitrage into one blockchain transaction to realize atomic implementations. These n trades will be executed atomically, and no other transactions can be inserted in the middle of them. Moreover, during the execution of smart contract, if some conditions have not been met, then Ethereum allows the smart contract to cancel the execution and revert the system state.

Our first observation of the arbitrage implementation is that 292,518 cyclic transactions are submitted within a single blockchain transaction and execute atomically, while only 88 cyclic arbitrages are conducted sequentially with different blockchain transactions, which indicates that atomic implementation of cyclic arbitrage dominates the entire market.

Because the order of blockchain transaction execution is determined by miners, there might be some other transactions executing in the middle of arbitrage trades if they are submitted separately. These external transactions might change the market price during the arbitrage process and generate the price impact. Consequently, 46 out of 88 sequential implementations of cyclic arbitrage have a negative revenue. In the scenario of cyclic arbitrage within a single transaction, if the output of the last trades is smaller than the input of the first trade because of the price impact of other transactions before the arbitrage execution, the execution of the n trades can be canceled, while the market states are reverted to those before the arbitrage. Although traders still pay the gas fee to the miner, they do not lose additional money for the non-profitable trades. Only 0.3% of atomic implementations have a negative revenue, which has a better performance than sequential implementations (52.3% of transactions have negative revenue).

Successful rate of atomic implementations: If the output of the cyclic transaction is smaller than the input, then the smart contract can cancel the execution of the transaction and result in a failed transaction recorded in the blockchain. Traders also need to pay a gas fee to miners for these failed transactions, which should be considered as the cost of cyclic arbitrage. Therefore, we investigate the success rate of atomic implementations.

For all failed transactions, there is no *Swap* event recorded in the blocks. Therefore, it is challenge to determine whether the transaction is aimed at cyclic arbitrage. We consider two methods to construct an upper bound and a lower bound for the success rate for each trader. For the lower bound, we just simply assume that all failed transactions issued by the traders who have ever placed a cyclic transaction are failed implementations of cyclic arbitrage. For the upper bound, we use a replay algorithm to evaluate all failed transactions [39]. As the cyclic transaction might be failed because of the price fluctuations between submitting and executing the cyclic

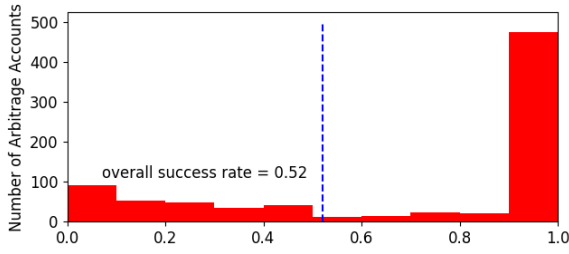


Figure 8: Lower bound of success rate of traders. The dotted line show the overall success rate of all traders.

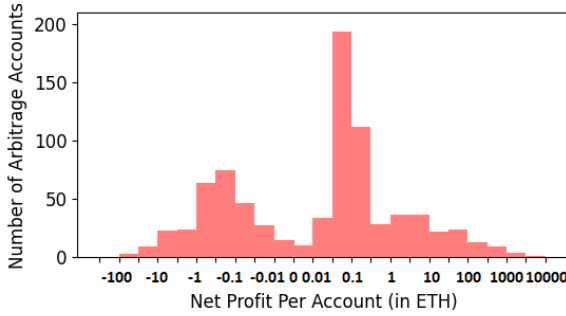


Figure 9: Lower bound of net profit of traders.

transaction, we replay the failed transaction upon its previous block state. If the result of replaying the failed transaction with a non-influenced market state is a cyclic transaction, then we determine it as a failed implementation of cyclic arbitrage. With the upper and lower bounds, we can estimate the success rate of atomic implementations.

In general, traders conduct atomic implementations with two methods: deploying a private smart contract to call exchange functions of Uniswap (282,563 transactions, 840 smart contracts) and directly calling the Uniswap public smart contract (9,955 transactions). Because each trader may have several different EOAs, while only authenticated EOAs can call private smart contracts, we consider all EOAs who use the same smart contract to perform cyclic arbitrage belong to the same trader.

Private smart contracts: We find that traders have called those private cyclic arbitrage smart contract 540,054 times in total and 282,563 successful transactions have been observed. The *lower bound* of the overall success rate is 52%, while most traders (475 out of 840) have a success rate higher than 90% (cf. Figure 8). If we consider the *upper bound* of success rates, then the overall success rate is 89.6% as only 34,236 failed transactions issued by arbitrage smart contracts can be recognized as cyclic transaction attempts with our replay experiments. The number of traders who have an upper bound success rate beyond 90% is 726. Figure 9 shows the distribution of the lower bounds of net profit of 840

smart contracts. The net profit (including failed attempts) of cyclic arbitrageurs is 21,360 ETH (upper bound: 25,742 ETH), while 66% (upper bound: 77.5%) of have a positive balance. Moreover, for those experienced traders who have performed more than 100 cyclic arbitrages, 119 (upper bound: 127) out of 129 traders have a positive net profit, suggesting that cyclic arbitrage is profitable over the long term for experienced traders.

Public smart contracts: Those traders who use public functions to perform cyclic transactions have a much lower success rate than those who deploy private smart contracts. Because the smart contract is public so we can decode their transactions although it is failed executed on the blockchain, which provides us an accurate success rate. They made 36,492 arbitrage attempts interacting with the Uniswap smart contract, yielding a success rate of 27.3% (9,955 out of 36,492). Moreover, traders cost 224 ETH as gas fees for failed transactions, which is much higher than their cyclic arbitrage profit (192 ETH) with the public smart contract.

Remarks: Atomic implementations of cyclic arbitrage provide two advantages over sequential implementations. First, traders can ensure the completeness of their arbitrage transactions. Either all trades will be executed, or none of them will be executed. Although we only find 88 complete cyclic arbitrage with sequential implementations, there might be more attempts which are failed in the middle of the process and cannot be identified by us. Second, if the cycle is not profitable at the time of the transaction execution, the smart contract can revert to the state when the cyclic trades have not been executed, which mitigates the financial loss when conducting cyclic arbitrage. These two advantages motivate traders to implement arbitrage transactions atomically with smart contracts.

Regarding the failure of cyclic transactions, there can be two reasons: the price impact and front-running attacks [14]. Some traders copy others' arbitrage strategies by observing these transactions in the blockchain P2P network and then create their own transactions in front of the original one to grab the benefits. By noticing the significant difference in the success rate, we may conjecture that the resistance to front-running determines the success rate of the private and public smart contracts as the price impact can be considered common to all traders. However, this conjecture needs to be validated more precisely.

7 CONCLUSION

In this paper, we provide a systematic study on cyclic arbitrage in AMM DEXes, including the arbitrage model, arbitrage opportunities, arbitrage markets, and arbitrage implementations. Additional to understanding cyclic arbitrages in DEXes, this paper also provides insights into two other areas.

We compare the arbitrage markets in DEXes and CEXes and discuss the differences between the two exchanges, which may benefit further study in understanding trader behaviors in cryptocurrency markets. Second, we examine the advantages of smart contract technologies in DEXes markets, which may inspire further studies to explore how traders may utilize blockchain technologies in financial markets.

This paper focuses on the fundamental understandings of cyclic arbitrage in DEXes and raises many interesting and important questions. For example: how do traders decide their strategies; how traders' strategies are affected by average gas fees and over-time variation in congestion; how do cyclic arbitrages influence other market participants; and how do traders combine utilize other services in the blockchain ecosystem to exploit cyclic arbitrage opportunities? We would like to investigate these follow up research questions in future work to promote understanding of user behaviors in the blockchain ecosystem.

REFERENCES

- [1] 2021. Alpha Homora V2. <https://alphafinancelab.gitbook.io/alpha-homora-v2/>. (2021).
- [2] 2021. DEX Ranking. <https://debank.com/ranking/dex?chain=eth>. (2021).
- [3] 2021. Gross Value Locked (USD). https://debank.com/ranking/locked_value. (2021).
- [4] 2021. The SushiSwap Project. <https://sushiswapchef.medium.com/the-sushiswap-projectdd6eb80c6ba2>. (2021).
- [5] 2021. Token Tracker ERC-20. <https://etherscan.io/tokens>. (2021).
- [6] 2021. Uniswap Analytics. <https://v2.info.uniswap.org/home>. (2021).
- [7] Hayden Adams. 2020. *Uniswap V2 Overview*. Technical Report. Uniswap.
- [8] Susan Athey, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia. 2016. Bitcoin pricing, adoption, and usage: Theory and evidence. (2016).
- [9] Zeta Avarikioti, Lioba Heimbach, Yuyi Wang, and Roger Wattenhofer. 2020. Ride the lightning: The game theory of payment channels. In *International Conference on Financial Cryptography and Data Security*. Springer, 264–283.
- [10] Sanghyun Bai and Fred Robinson. 2019. Automated Triangular Arbitrage: A Trading Algorithm for Foreign Exchange on a Cryptocurrency Market. (2019).
- [11] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives* 29, 2 (2015), 213–38.
- [12] Weili Chen, Tuo Zhang, Zhiguang Chen, Zibin Zheng, and Yutong Lu. 2020. Traveling the token world: A graph analysis of ethereum erc20 token ecosystem. In *Proceedings of The Web Conference 2020*. 1411–1421.
- [13] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2019. Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges. *arXiv preprint arXiv:1904.05234* (2019).
- [14] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 910–927.
- [15] David Easley, Maureen O'Hara, and Soumya Basu. 2019. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics* 134, 1 (2019), 91–109.
- [16] Ittay Eyal. 2015. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy*. IEEE, 89–103.
- [17] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*. Springer, 436–454.
- [18] Christof Ferreira Torres, Ramiro Camino, et al. 2021. Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain. In *USENIX Security Symposium, Virtual 11-13 August 2021*.
- [19] Henry N Goldstein. 1964. The implications of triangular arbitrage for forward exchange policy. *The Journal of Finance* 19, 3 (1964), 544–551.
- [20] Paz Grimberg, Tobias Lauinger, and Damon McCoy. 2020. Empirical analysis of indirect internal conversions in cryptocurrency exchanges. *arXiv preprint arXiv:2002.12274* (2020).
- [21] Campbell R Harvey. 2016. Cryptofinance. *Available at SSRN 2438299* (2016).
- [22] Campbell R Harvey, Ashwin Ramachandran, and Joey Santoro. 2021. *DeFi and the Future of Finance*. John Wiley & Sons.
- [23] Gur Huberman, Jacob Leshno, and Ciamac C Moallemi. 2017. Monopoly without a monopolist: An economic analysis of the bitcoin

- payment system. *Bank of Finland Research Discussion Paper* 27 (2017).
- [24] Aggelos Kiayias, Elias Koutsoupias, Maria Kyropoulou, and Yiannis Tselekounis. 2016. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*. 365–382.
 - [25] Elias Koutsoupias, Philip Lazos, Foluso Ogunlana, and Paolo Serafino. 2019. Blockchain mining games with pay forward. In *The World Wide Web Conference*. 917–927.
 - [26] Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, and Yongdae Kim. 2017. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 195–209.
 - [27] Robert Leshner and Geoffrey Hayes. 2019. Compound Finance Whitepaper.
 - [28] Michael Lewis. 2014. *Flash boys: a Wall Street revolt*. WW Norton & Company.
 - [29] Bowen Liu, Pawel Szalachowski, and Jianying Zhou. 2020. A first look into defi oracles. *arXiv preprint arXiv:2005.04377* (2020).
 - [30] Hanqing Liu, Na Ruan, Rongtian Du, and Weijia Jia. 2018. On the strategy and behavior of bitcoin mining with n-attackers. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 357–368.
 - [31] Igor Makarov and Antoinette Schoar. 2020. Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics* 135, 2 (2020), 293–319.
 - [32] Francisco J Marmolejo-Cossio, Eric Brigham, Benjamin Sela, and Jonathan Katz. 2019. Competing (semi-) selfish miners in Bitcoin. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. 89–109.
 - [33] Frank McCormick. 1979. Covered interest arbitrage: unexploited profits? Comment. *Journal of Political Economy* 87, 2 (1979), 411–417.
 - [34] Zheng Nan and Taisei Kaizoji. 2019. Bitcoin-based triangular arbitrage with the Euro/US dollar as a foreign futures hedge: modeling with a bivariate GARCH model. *Quantitative Finance and Economics* 3, 2 (2019), 347–365.
 - [35] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. 2016. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 305–320.
 - [36] Emiliano Pagnotta and Andrea Buraschi. 2018. An equilibrium valuation of bitcoin and decentralized network assets. *Available at SSRN 3142022* (2018).
 - [37] Lukáš Pichl, Zheng Nan, and Taisei Kaizoji. 2020. Time series analysis of ether cryptocurrency prices: Efficiency, predictability, and arbitrage on exchange rates. In *Advanced studies of financial technologies and cryptocurrency markets*. Springer, 183–196.
 - [38] Kaihua Qin, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti, and Arthur Gervais. 2021. CeFi vs. DeFi—Comparing Centralized to Decentralized Finance. *arXiv preprint arXiv:2106.08157* (2021).
 - [39] Kaihua Qin, Liyi Zhou, and Arthur Gervais. 2021. Quantifying Blockchain Extractable Value: How dark is the forest? *arXiv preprint arXiv:2101.05511* (2021).
 - [40] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. 2021. Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. In *International Conference on Financial Cryptography and Data Security*. Springer.
 - [41] Geoffrey Ramseyer, Ashish Goel, and David Mazieres. [n. d.]. Scaling On-Chain Asset Exchanges via Arrow-Debreu Exchange Markets. ([n. d.]).
 - [42] Ayelet Sapirshtein, Yonatan Sompolsky, and Aviv Zohar. 2016. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, 515–532.
 - [43] Ye Wang, Lioba Heimbach, and Roger Wattenhofer. 2021. Behavior of Liquidity Providers in Decentralized Exchanges. *arXiv preprint arXiv:2105.13822* (2021).
 - [44] Gavin Wood et al. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151, 2014 (2014), 1–32.
 - [45] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2021. High-frequency trading on decentralized on-chain exchanges. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 428–445.

A EXISTENCE OF CYCLIC ARBITRAGE OPPORTUNITIES

Theorem 1. For a given cycle $A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n \rightarrow A_1$ with n tokens, there exists an arbitrage opportunity for the cyclic transaction if the product of exchange rates $\frac{a_{2,1} \cdot a_{3,2} \cdot \dots \cdot a_{1,n}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,1}} > \frac{1}{r_1^n \cdot r_2^n}$, where $a_{i,j}$ denotes the liquidity of token A_i in the liquidity pool with token A_j . Meanwhile, the arbitrage cannot benefit from the reversed direction $A_1 \rightarrow A_n \rightarrow \dots \rightarrow A_2 \rightarrow A_1$ for cyclic transactions.

We first give a general expression of cyclic transactions with more than three tokens.

LEMMA 2. For a cyclic transaction through a path with n edges $A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n \rightarrow A_1$, the first deviation of the utility function at $\delta_1 = 0$ is $\frac{\partial U}{\partial \delta_1} \Big|_{\delta_1=0} = \frac{r_1^n \cdot r_2^n \cdot a_{1,n} \cdot a_{2,1} \cdot \dots \cdot a_{n,n-1}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,1}} - 1$.

PROOF. We can observe that the transaction through $A_1 \rightleftharpoons A_2$ and $A_2 \rightleftharpoons A_3$ is equivalent to an exchange of δ_1 through liquidity pool $A'_1 \rightleftharpoons A'_3$, where $a'_{1,3} = \frac{a_{1,2} \cdot a_{2,3}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}$, and $a'_{3,1} = \frac{r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,2}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}$.

We prove this lemma by induction. We first show it is correct when $n = 3$.

We take the utility function of a cyclic transaction of three tokens and compute the first deviation of the function,

$$\frac{\partial U_{A_1 A_2 A_3 A_1}}{\partial \delta_1} \Big|_{\delta_1=0} = \frac{r_1^3 \cdot r_2^3 \cdot a_{1,3} \cdot b_{2,1} \cdot b_{3,2}}{a_{1,2} \cdot a_{2,3} \cdot b_{3,1}} - 1 \quad (1)$$

For $n \geq 3$, the inductive hypothesis is that the equation is true for n :

$$\frac{\partial U}{\partial \delta_1} \Big|_{\delta_1=0} = \frac{r_1^n \cdot r_2^n \cdot a_{1,n} \cdot a_{2,1} \cdot \dots \cdot a_{n,n-1}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,1}} - 1.$$

The inductive step is to prove the equation for $n + 1$:

If we exchange δ_1 through $A_1 \rightleftharpoons A_2$ pool to get δ_2 , and obtain δ_3 from $A_2 \rightleftharpoons A_3$ by trading δ_2 right after, these two atomic transactions can be equivalent to a single transaction with δ_1 in a virtual pool $A'_1 \rightleftharpoons A'_3$, where $a'_{1,3} = \frac{a_{1,2} \cdot a_{2,3}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}$, and $a'_{3,1} = \frac{r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,2}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}$.

We assume that the statement is correct for any n -path cyclic transaction. Consider a cyclic transaction through a $n + 1$ -path $A_1 \rightarrow A^2 \rightarrow \dots \rightarrow A_n \rightarrow A_{n+1} \rightarrow A_1$, which is equivalent to a n -path cyclic transaction through $A'_1 \rightarrow A'_3 \rightarrow \dots \rightarrow A_{n+1} \rightarrow A'_1$, where the first deviation of the utility function at $\delta_1 = 0$ is,

$$\begin{aligned} \frac{\partial U}{\partial \delta_1} \Big|_{\delta_1=0} &= \frac{r_1^n \cdot r_2^n \cdot a_{1,n+1} \cdot a'_{3,1} \cdot \dots \cdot a_{n+1,n}}{a'_{1,3} \cdot a_{3,4} \cdot \dots \cdot a_{n+1,1}} - 1 \\ &= \frac{r_1^n \cdot r_2^n \cdot a_{1,n+1} \cdot \frac{r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,2}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}} \cdot \dots \cdot a_{n+1,n}}{\frac{a_{1,2} \cdot a_{2,3}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}} \cdot a_{3,4} \cdot \dots \cdot a_{n+1,1}} - 1 \quad (2) \\ &= \frac{r_1^{n+1} \cdot r_2^{n+1} \cdot a_{1,n+1} \cdot a_{2,1} \cdot \dots \cdot a_{n+1,n}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n+1,1}} - 1 \end{aligned}$$

By the principle of mathematical induction: the first deviation of the utility function at $\delta_a = 0$ is $\frac{r_1^{n+1} \cdot r_2^{n+1} \cdot a_{1,n+1} \cdot a_{2,1} \cdot \dots \cdot a_{n+1,n}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n+1,1}} - 1$, for any $n \geq 3$. \square

PROOF OF THEOREM 1. Assume that we would like to exchange δ_1 of token A_1 through the cycle. When $\delta_1 = 0$, both the value of $U_{A_1 A_2 A_n A_1}$ and the value of $U_{A_1 A^n A^2 A_1}$ are 0.

Then we consider the first and the second derivative of the utility function at $\delta_1 = 0$.

$$\frac{\partial U_{A_1 A_2 A_n A_1}}{\partial \delta_1} \Big|_{\delta_1=0} = \frac{r_1^n \cdot r_2^n \cdot a_{1,n} \cdot a_{2,1} \cdot \dots \cdot a_{n,n-1}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,1}} - 1 \quad (3)$$

If arbitrageurs can make profit in this trading direction, then,

$$\begin{aligned} 0 &< \frac{\partial U_{A_1 A_2 A_n A_1}}{\partial \delta_1} \Big|_{\delta_1=0} \\ \frac{1}{r_1^n \cdot r_2^n} &< \frac{a_{1,n} \cdot a_{2,1} \cdot \dots \cdot a_{n,n-1}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,1}} \end{aligned} \quad (4)$$

which implies that $\frac{r_1^n \cdot r_2^n \cdot a_{1,n} \cdot a_{2,1} \cdot \dots \cdot a_{n,n-1}}{a_{1,2} \cdot a_{2,3} \cdot \dots \cdot a_{n,n-1}} < 1$,

then $\frac{\partial U_{A_1 A_n A_2 A_1}}{\partial \delta_1} \Big|_{\delta_1=0} < 0$.

By computing the second derivative of $U_{A_1 A_n A_2 A_1}$, we know that $\frac{\partial^2}{\partial \delta_1^2} U_{A_1 A_n A_2 A_1}$ is negative for all $\delta_1 \in \mathbb{R}^+$. $U_{A_1 A_n A_2 A_1}$ is a monotone decreasing function in its domain, and the maximum value of $U_{A_1 A_n A_2 A_1}$ is 0 at $\delta_1 = 0$. Therefore, there is no opportunity for arbitrage through the reversed direction $A_1 \rightarrow A^n \rightarrow \dots \rightarrow A^2 \rightarrow A_1$ for cyclic transactions.

Arbitrageurs cannot benefit from trading δ_1 through $A_1 \rightarrow A^n \rightarrow \dots \rightarrow A^2 \rightarrow A_1$, sequentially. Therefore, arbitrageurs have at most one direction to benefit themselves with cyclic transactions. \square

B OPTIMAL TRADE VOLUME

We start from a simple case where cyclic transactions happen in a cycle of token A_1 , A_2 , and A_3 . We denote $a_{i,j}$ as the liquidity of token A_i in the liquidity pool with token A_j . If we directly exchange A_3 with δ_1 of A_1 , then we receive the

研究 private smart contract.

output amount of A_3 , $\delta_3 = \frac{r_1 \cdot r_2 \cdot a_{3,1} \cdot \delta_1}{a_{1,3} + r_1 \cdot \delta_1}$. If we take token A_2 as an intermediate, then the output amount of A_3 is $\delta'_3 =$

$\frac{r_1^2 \cdot r_2^2 \cdot a_{2,1} \cdot a_{3,2} \cdot \delta_1}{a_{1,2} \cdot a_{2,3} + r_1 \cdot \delta_1 \cdot (a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1})}$. Compare δ_3 and δ'_3 , δ'_3 can be written in the format as

$\delta'_3 = \frac{r_1 \cdot r_2 \cdot \frac{r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,2}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}} \cdot \delta_1}{\frac{a_{1,2} \cdot a_{2,3}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}} + r_1 \cdot \delta_1}$. Therefore, this transaction through

two pools can be considered as a transaction through an equivalent pool of A_1 and A_3 where the liquidity of A_1 is $a'_{1,3} = \frac{a_{1,2} \cdot a_{2,3}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}$ and the liquidity of A_3 is $a'_{3,1} = \frac{r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,2}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}$.

Then, we can rewrite the utility function of a cyclic transaction in $A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow A_1$ with input δ_1 as

$$U_{A_1 A_2 A_3 A_1} = \left(\frac{r_1 \cdot r_2 \cdot \frac{r_1 \cdot r_2 \cdot a_{2,1} \cdot a_{3,2}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}}}{\frac{a_{1,2} \cdot a_{2,3}}{a_{2,3} + r_1 \cdot r_2 \cdot a_{2,1}} + r_1 \cdot \delta_1} - 1 \right) \cdot \delta_1 \quad (5)$$

Let us denote $a = \frac{a'_{1,3} \cdot a_{3,1}}{a_{3,1} + r_1 \cdot r_2 \cdot a'_{3,1}}$ and $a' = \frac{r_1 \cdot r_2 \cdot a_{1,3} \cdot a'_{3,1}}{a_{3,1} + r_1 \cdot r_2 \cdot a'_{3,1}}$

$$\begin{aligned} \frac{\partial U_{A_1 A_2 A_3 A_1}}{\partial \delta_a} &= \frac{r_1 \cdot r_2 \cdot a' \cdot (a + r_1 \cdot \delta_1) - r_1 \cdot (r_1 \cdot r_2 \cdot a' \cdot \delta_1)}{(a + r_1 \cdot \delta_1)^2} - 1 \\ \frac{\partial U_{A_1 A_2 A_3 A_1}}{\partial \delta_a} &= \frac{r_1 \cdot r_2 \cdot a' \cdot a}{(a + r_1 \cdot \delta_1)^2} - 1 \end{aligned} \quad (6)$$

To maximize the utilize, we have $\frac{\partial U_{A_1 A_2 A_3 A_1}}{\partial \delta_1} = 0$, therefore,

$$\begin{aligned} \frac{r_1 \cdot r_2 \cdot a' \cdot a}{(a + r_1 \cdot \delta_1)^2} - 1 &= 0 \\ r_1 \cdot r_2 \cdot a' \cdot a &= (a + r_1 \cdot \delta_1)^2 \\ \delta_1 &= \frac{\sqrt{r_1 \cdot r_2 \cdot a' \cdot a} - a}{r_1} \end{aligned} \quad (7)$$

We can find the equivalent pool of transactions for longer paths between any pair of tokens iteratively as in the first step of computing pools equivalent to $A_1 \rightleftharpoons A_2$ and $A_2 \rightleftharpoons A_3$ and then determine the optimal input of the cyclic transaction.