

Multi-Path Routing Algorithm for Cost-Effective Transactions in Automated Market Makers

Hyun Bin Jeong[†] · Soo Young Park^{**}

ABSTRACT

With the rise of a decentralized finance market (so called, DeFi) using blockchain technology, users and capital liquidity of decentralized finance applications are increasing significantly. The Automated Market Maker (AMM) is a protocol that automatically calculates the asset price based on the liquidity of the decentralized trading platform, and is currently most commonly used in the decentralized exchanges (DEX), since it can proceed the transactions by utilizing the liquidity pool of the trading platform even if the buyers and sellers do not exist at the same time. However, Automated Market Maker have some disadvantages since the cost efficiency of each transaction using Automated Market Maker depends on the liquidity size of some liquidity pools used for the transaction, so the smaller the size of the liquidity pool and the larger the transaction size, the smaller the cost efficiency of the trade. To solve this problem, some platforms are adopting Transaction Path Routing Algorithm that bypasses transaction path to other liquidity pools that have relatively large size to improve cost efficiency, but this algorithm can be further improved because it uses only a single transaction path to proceed each transaction. In addition to just bypassing transaction path, in this paper we proposed a Multi-Path Routing Algorithm that uses multiple transaction paths simultaneously by distributing transaction size, and showed that the cost efficiency of transactions can be further improved in the Automated Market Maker-based trading environment.

Keywords : Blockchain, Decentralized Finance, Automated Market Maker

자동화 마켓 메이커에서 비용 효율적인 거래를 위한 다중 경로 라우팅 알고리즘

정 현 빈[†] · 박 수 용^{**}

요 약

블록체인 기반 탈중앙화 금융 시장의 등장과 함께 분산 금융 어플리케이션의 사용자와 자본 유동성이 크게 증가하고 있다. 자동화 마켓 메이커는 탈중앙화 거래 플랫폼의 유동성을 바탕으로 자동으로 거래 단가를 계산하는 프로토콜로, 거래 플랫폼의 유동성 풀을 활용하여 구매자와 판매자가 동 시간대에 존재하지 않아도 거래의 성사를 가능하게 하여 현재 탈중앙화 거래 시장에서 가장 일반적으로 사용되고 있다. 그러나 자동화 마켓 메이커는 거래의 비용 효율이 거래에 사용되는 특정 유동성 풀의 유동성 규모에 의존하여, 유동성 풀의 규모가 작고 거래의 규모가 클수록 거래의 비용 효율이 크게 감소한다는 단점이 있다. 이를 해결하기 위한 방법으로 상대적으로 유동성의 규모가 큰 유동성 풀로 거래 경로를 우회하여 비용 효율을 개선하는 거래 경로 라우팅 알고리즘이 채택되고 있지만, 단일 거래 경로만을 사용하기 때문에 여전히 개선의 여지가 존재한다. 본 논문에서는 거래 경로를 우회하는 것에 더하여 거래 규모를 분산하여 다수의 거래 경로를 동시에 탐색하는 다중 경로 라우팅 알고리즘을 제안하고, 해당 알고리즘을 사용하여 자동화 마켓 메이커 기반의 거래 환경에서 기존의 거래 경로 라우팅 알고리즘에 비해 거래의 비용 효율을 개선한다.

키워드 : 블록체인, 탈중앙화 금융, 자동화 마켓 메이커

1. 서 론

이더리움을 비롯하여 스마트 컨트랙트를 지원하는 블록체

인 플랫폼의 사용자가 증가함에 따라 기존의 중앙화된 거래 환경을 탈중앙화 하려는 시도가 증가하고 있다. 초기의 블록체인 기반 탈중앙화 거래소들은 오더북(order book) 방식의 거래 환경을 채택하였는데, 이는 거래의 매수 주문이나 매도 주문, 거래 취소 주문 등 사용자가 취할 수 있는 모든 행동에 대해 블록체인 플랫폼의 사용료인 트랜잭션 가스비(transaction gas fee)를 지불해야 한다는 번거로움이 있었다[1]. 특히 거래 가격의 변동성이 높은 자산의 경우 잦은 주문 취

※ 이 논문은 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터 지원사업의 연구결과로 수행되었음.

† 비 회 원 : 서강대학교 컴퓨터공학과 석사

** 정 회 원 : 서강대학교 컴퓨터공학과 교수 및 지능형블록체인센터 센터장

Manuscript Received : March 2, 2022

Accepted : April 4, 2022

* Corresponding Author : Soo Young Park(sypark@sogang.ac.kr)

소와 재 주문 등의 행동을 필요로 하기 때문에 탈중앙화 거래소에서 오더북 방식은 일반 사용자들의 접근성을 낮추는 진입장벽으로 작용하였다[2].

자동화 마켓 메이커(Automated Market Maker)[3]는 거래소에 유입되어 있는 유동성을 바탕으로 자동으로 거래 단가를 계산하는 프로토콜로, 매수자의 매수 주문과 매도자의 매도 주문이 매칭되어야 거래가 성사되는 오더북 방식과 달리 자동화 마켓 메이커는 매수자 또는 매도자가 제출하는 거래 규모에 따라 계산한 거래 단가로 거래를 성사시킨다. 사전에 공급되어 있는 자산 유동성이 거래 상대방의 역할을 대신하기 때문에 매수자와 매도자가 동시에 존재하지 않아도 거래를 진행할 수 있고, 하나의 매수 또는 매도 주문으로도 거래가 체결되기 때문에 가스비의 부담도 덜하다는 장점이 있어 현재 많은 탈중앙화 거래소에서 오더북 대신 자동화 마켓 메이커를 사용한 거래 환경을 채택하고 있다[4]. 오더북 방식에 비해 거래가 간편하고 가스비의 부담도 덜하기 때문에 자동화 마켓 메이커를 채택한 거래 플랫폼이 증가하면서 탈중앙화 금융(Decentralized Finance, DeFi) 시장의 성장도 탄력을 받기 시작하였는데, 해당 시장에 꾸준히 유동성이 유입된 결과 탈중앙화 금융 시장의 규모를 직관적으로 파악하기 위해 일반적으로 사용되는 지표인 TVL(Total Value Locked)이 2021년 상반기에 1천억 달러를 넘어서게 되었다 [5]. Fig. 1은 2019년부터 2021년까지 탈중앙화 금융 시장의 TVL 변화를 나타낸 것이다.

자동화 마켓 메이커는 현재 탈중앙화 거래 플랫폼에서 가장 일반적으로 쓰이고 있는 프로토콜이지만 몇 가지 단점도 존재한다. 자동화 마켓 메이커 기반의 거래 플랫폼에서는 거래의 비용 효율(cost efficiency)이 거래의 규모와 거래에 사용되는 유동성 풀의 규모에 의존하는데, 특히 거래의 규모가 크고 유동성 풀의 규모가 작을수록 거래의 비용 효율이 크게 감소한다. 또한 자동화 마켓 메이커가 거래 단가를 자

동으로 계산하고 간편한 거래 환경을 제공하기 위한 자본의 유동성이 유동성 풀(liquidity pool)의 형태로 사전에 해당 거래 플랫폼에 공급될 필요가 있는데, 시장의 관심이 낮은 등의 이유로 평소 거래 볼륨이 낮은 자산의 경우에는 해당 자산의 거래에 사용되기 위해 유입된 유동성이 실제로 사용되는 빈도가 낮아 유동성 풀이 사용되지 않는 기간이 생기기도 한다.

탈중앙화 금융 시장에서 처음으로 자동화 마켓 메이커를 채택하였으며 현재 가장 높은 인지도와 사용자층을 확보한 유니스왑(Uniswap)은 거래 경로 라우팅 알고리즘(Transaction Path Routing Algorithm, Uniswap Router)을 도입하여 이 문제를 해결하고자 하였다[6]. 거래 경로 라우팅 알고리즘은 자산의 거래에 사용되는 유동성 풀의 규모가 거래 규모에 비해 작은 등의 이유로 거래의 비용 효율이 낮을 것으로 예상되는 경우 필요에 따라 상대적으로 유동성의 규모가 큰 풀로 거래 경로를 우회하여 비용 효율을 개선하는데, 이러한 장점 덕분에 현재 유니스왑을 따라 많은 탈중앙화 거래 플랫폼들이 거래 경로 라우팅 알고리즘을 조금씩 도입하여 사용하고 있다. 하지만 유니스왑을 비롯하여 이 거래 플랫폼들이 사용하는 거래 경로 라우팅 알고리즘은 항상 단일 거래 경로만을 사용하기 때문에 여전히 거래의 비용 효율을 개선할 수 있는 여지가 존재하는데, 이러한 관점에 착안하여 본 논문에서는 단순히 단일 거래 경로를 사용하는 것에 더하여 다수의 거래 경로를 동시에 사용하는 것을 고려하는 다중 경로 라우팅 알고리즘(Multi-Path Routing Algorithm)을 제안한다. 다중 경로 라우팅 알고리즘은 필요에 따라 최대 3개의 경로로 거래 규모를 적절히 분산하는 최적의 거래 경로를 도출하며, 본 논문에서 제안하는 해당 알고리즘을 통해 자동화 마켓 메이커 기반의 탈중앙화 거래 환경에서 기존의 단일 경로 라우팅 알고리즘에 비해 거래의 비용 효율을 더욱 개선할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 자동화 마켓 메이커의 등장 배경에 대해 소개하고, 본 논문에서 제안하는 알고리즘의 성능을 평가하는 기준인 거래의 효율에 대해 소개한 뒤, 유니스왑에 대한 기본적인 배경지식을 소개한다. 3장에서는 유니스왑을 비롯하여 현재 탈중앙화 거래 플랫폼에서 가장 많이 사용되는 자동화 마켓 메이커의 한 종류인 상수곱 마켓 메이커에 대해 설명한 뒤, 유니스왑에서 처음으로 도입한 거래 경로 라우팅 알고리즘에 대해 설명한다. 4장에서는 본 논문에서 제안하는 다중 경로 라우팅 알고리즘의 아이디어와 구체적인 동작 방식에 대해 설명한다. 5장에서는 다중 경로 라우팅 알고리즘을 실제 유동성 풀 데이터를 기반으로 한 시뮬레이션 환경에서 기존의 거래 경로 라우팅 알고리즘, 즉 단일 경로 라우팅 알고리즘과 비교하는 실험을 진행한 결과를 분석한다. 6장에서는 본 논문의 결론과 향후 연구에 대해 설명한다.

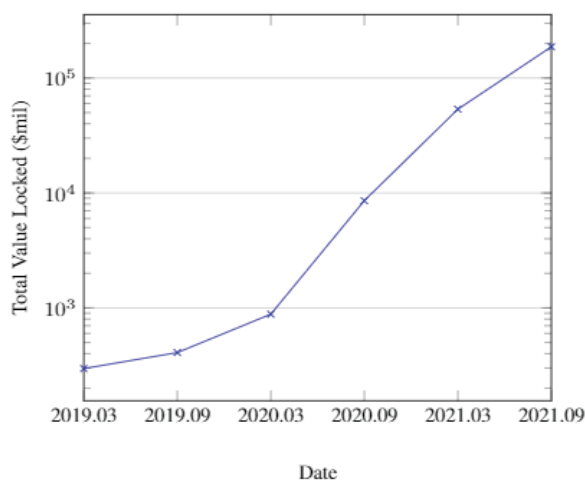


Fig. 1. Decentralized Finance Market TVL

2. 배경지식

본 장에서는 본 논문의 연구 배경이 되는 자동화 마켓 메이커와 비용 효율의 개념 및 유니스왑에 대해 소개한다.

2.1 자동화 마켓 메이커

자동화 마켓 메이커는 자산의 거래 플랫폼에 유입되어 있는 유동성을 바탕으로 거래자의 거래 규모에 따라 자동으로 거래 단가를 계산하는 프로토콜이다. 매수자와 매도자가 같은 거래 단가에 합의해야 거래가 성사되는 기존의 거래 방식인 오더북 방식과 상반되는 이러한 개념 자체는 1990년 초에 시어슨 리먼 브라더스(Sheason Lehman Brothers)에 의해 고안되었다고 알려져 있지만, 이를 블록체인에 적용하는 것을 제안한 것은 이더리움의 창시자인 비탈릭 부테린이다. 기존에 사용되던 이더리움 기반의 탈중앙화 거래소들은 모두 오더북 방식을 사용하고 있었는데, 비탈릭 부테린은 이더리움과 같이 각 트랜잭션에 대해 사용료를 지불하는 블록체인 플랫폼에서 오더북 방식을 사용하는 것이 상당한 비용을 발생시킨다는 문제를 제기하였고, 이에 대한 해결책으로 자동화 마켓 메이커를 사용하는 것을 제안하였다[7].

블록체인 기반의 탈중앙화 거래소에서 자동화 마켓 메이커가 거래 규모에 따라 자산의 거래 단가를 계산하기 위해서는 사전에 해당 거래 플랫폼에 적절한 유동성이 공급되어 있어야 하는데, 이러한 유동성이 각 자산의 거래 페어별로 모여있는 것을 유동성 풀이라 한다. 예를 들어 ETH와 USDT 두 자산 간의 거래를 위해서는 ETH와 USDT의 유동성이 공급되어 있는 ETH/USDT 유동성 풀이 필요하다.

ETH와 USDT 간의 거래를 위해 두 자산의 유동성이 공급되어 있는 ETH/USDT 유동성 풀이 필요한 것처럼, 자동화 마켓 메이커를 채택한 거래 플랫폼은 서로 거래가 가능한 각 자산들이 페어를 이루고 있는 각각의 유동성 풀들을 필요로 한다. 이러한 조건을 보다 쉽게 충족하기 위한 방법으로 자동화 마켓 메이커를 채택한 탈중앙화 거래 플랫폼은 일반 사용자들이 자신의 의사에 따라 직접 유동성 풀에 유동성을 공급할 수 있도록 하고 있는데, 더 많은 사람들이 유동성을 공급하도록 유도하기 위한 인센티브 모델로 거래 수수료 분배 모델을 도입하여 각 유동성 공급자들이 보유한 유동성 풀 내 지분에 따라 거래 수수료를 나누어 받을 수 있도록 하는 것이 일반적이다[8].

유동성 풀의 규모와 거래 규모에 따라 자산의 거래 단가를 계산하는 방법은 자동화 마켓 메이커가 어떤 마켓 메이킹 모델을 채택하고 있는가에 따라 상이한데, 현재 블록체인 기반의 탈중앙화 거래 시장에서는 거래의 전후로 유동성 풀 내 각 자산의 수량의 곱을 일정하게 유지하도록 거래를 처리하는 상수곱 마켓 메이커(Constant Product Market Maker,

CPMM)[9]를 사용하는 것이 일반적이며, 그 외에 알려져 있는 마켓 메이커는 유동성 풀 내 각 자산의 수량의 합을 일정하게 유지하도록 거래를 처리하는 상수합 마켓 메이커(Constant Sum Market Maker, CSMM)[10] 등이 있다.

2.2 비용 효율

어떤 행동을 취할 때 수반되는 비용에 비하여 그 행동의 결과로부터 얻을 수 있는 효용이 충분히 높을 때 이를 비용 효율적(Cost-Effective)이라 하는데, 블록체인 기반의 탈중앙화 거래 시장에서 비용 효율이라는 개념과 의미는 다소 상반되지만 유사한 관점에서 쓰이는 용어로 Price Impact가 있다. Price Impact란 두 자산 간의 거래에 의해 유동성 풀을 구성하는 각 자산의 비율이 변하는 정도를 말하며, 좀 더 직관적으로는 자산의 거래가 해당 자산의 가격에 미치는 영향이라고 표현할 수 있다. 예를 들어 ETH를 USDT로 교환하고자 하는 어떤 거래자가 제출한 주문에 의해 거래가 성사되어 ETH/USDT 유동성 풀 내 ETH의 수량이 늘어나고 USDT의 수량이 줄어들 때, 그 비율이 1 ETH당 4000 USDT (4000 USDT/ETH) 에서 1 ETH당 3600 USDT (3600 USDT/ETH) 로 바뀌었다면 해당 거래의 Price Impact는 10%가 된다.

거래의 Price Impact가 클 수록 해당 거래의 주문을 제출하는 거래자가 감수하는 비용도 높아지기 때문에 탈중앙화 거래 시장에서 Price Impact는 거래자가 거래를 주문할 때 감수하는 비용을 직관적으로 알 수 있는 가장 일반적으로 쓰이는 용어이지만, 본 논문에서 제안하는 다중 경로 라우팅 알고리즘이 거래의 비용 효율을 개선할 수 있음을 실험을 통해 검증하는 것이 목적이기 때문에 본 논문에서는 Price Impact 대신 거래의 비용 효율 내지는 거래의 효율이라는 표현을 주로 사용하였다. 비용 효율이 더 높다는 것은 같은 비용을 지불할 때 비교 대상에 비해 더 높은 효용을 얻을 수 있음을 의미하고, 비용 효율이 더 낮다는 것은 반대로 비교 대상에 비해 같은 비용 대비 더 낮은 효용을 얻을 수 있음을 의미한다.

2.3 유니스왑

유니스왑은 자동화 마켓 메이커를 도입한 최초의 탈중앙화 거래 플랫폼으로, 오더북 방식을 쓰던 기존 탈중앙화 거래 플랫폼이 가진 문제점의 해결방안으로 자동화 마켓 메이커의 사용을 제안한 비탈릭 부테린의 의견을 참고하여 개발되었다고 알려져 있다. 유니스왑에서 채택한 마켓 메이킹 모델은 상수곱 마켓 메이커로, 자동화 마켓 메이커의 거래 처리 방식 특성상 충분한 규모의 유동성 풀이 구성될 필요가 있었기 때문에 유동성 공급자들에 대한 인센티브로서 0.3%의 거래 수수료 분배 모델을 적용하였다.

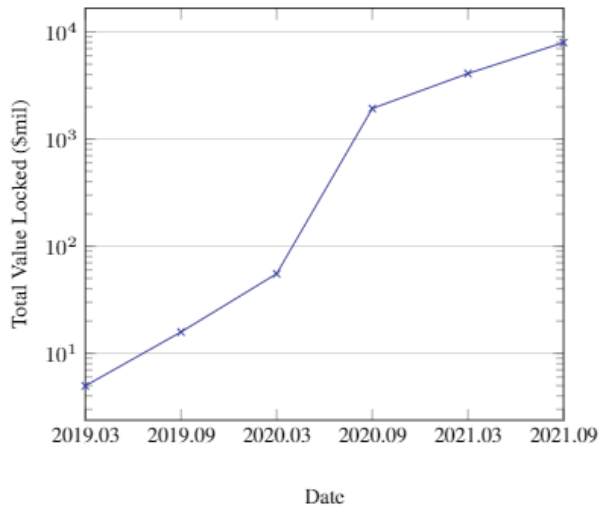


Fig. 2. Uniswap TVL

초기의 유니스왑은 자동화 마켓 메이커 기반의 가장 기본적인 형태의 거래만을 지원하였는데, 이 시기에는 탈중앙화 금융 시장에 대한 관심이 비교적 낮았기 때문에 부족한 유동성을 보완하기 위해 각 개별 자산의 거래 페어로 당시 이더리움(Ethereum) 플랫폼에서 가장 유동성이 풍부했던 자산인 이더리움(ETH)을 사용하는 것이 일반적이었다. 예를 들어 자산 A의 유동성은 A/ETH 페어의 형태로 A/ETH 유동성 풀에, 자산 B의 유동성은 B/ETH 페어의 형태로 B/ETH 유동성 풀에 공급되었고, 자산 A를 B로 교환하기 위해서는 A/ETH 풀을 통한 거래와, B/ETH 풀을 통한 거래를 각각 수행하는 방식이었다. 이후 탈중앙화 금융 시장에 대한 관심이 높아짐에 따라 이더리움 이외에 비트코인을 ERC20 토큰의 형태로 발행한 랩트비트코인(WBTC)[11] 및 USDT나 USDC와 같은 스테이블코인의 유통량이 크게 증가하여 유니스왑에 풍부한 유동성이 유입되었고, 그와 더불어 거래의 최적 경로를 탐색하여 제안하는 거래 경로 라우팅 알고리즘을 도입하는 등 몇 가지 업데이트를 적용하여 유니스왑에서 처리되는 거래의 전반적인 비용 효율이 개선되었다. Fig. 2는 2019년부터 2021년까지 유니스왑의 TVL 변화를 나타낸 것이다.

3. 관련 연구

본 장에서는 본 논문에서 제안하는 다중 경로 라우팅 알고리즘의 착안점이 되는 상수급 마켓 메이커와 유니스왑의 거래 경로 라우팅 알고리즘에 대해 설명한다.

3.1 상수급 마켓 메이커

자동화 마켓 메이커를 채택한 탈중앙화 거래 플랫폼에서

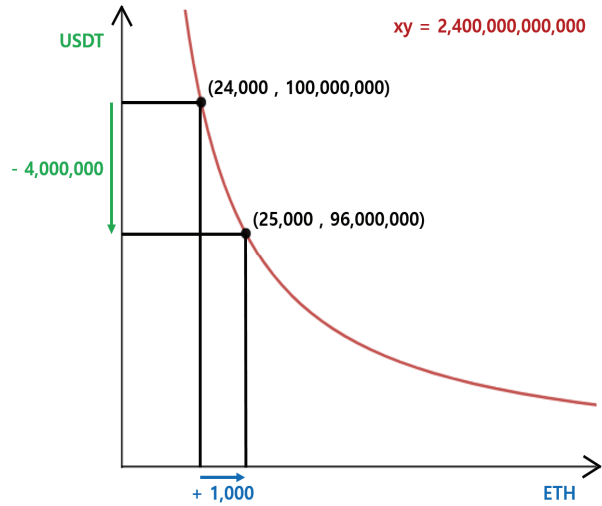


Fig. 3. Constant Product Market Maker Example

가장 흔하게 볼 수 있는 마켓 메이킹 모델인 상수급 마켓 메이커는 유동성 풀을 구성하는 두 자산 간의 거래 발생 시, 거래 전후로 두 자산의 수량의 곱이 변하지 않도록 유지한다는 원칙에 따라 거래를 처리한다. 상수급 마켓 메이커를 사용하는 거래 플랫폼의 유동성 풀 A/B에 공급되어 있는 자산 A와 B의 수량을 각각 α 와 β 라 할 때, x 개의 자산 A를 자산 B로 교환할 경우 받게 되는 자산 B의 수량 y 를 구하는 방법은 Equation (1)과 같다.

$$y = \beta - (\alpha \times \beta) / (\alpha + x) \tag{1}$$

구체적인 예를 들면 ETH/USD 유동성 풀에 24,000개의 ETH와 100,000,000개의 USD가 공급되어 있다고 가정할 경우, 어떤 거래자가 1,000개의 ETH를 USD로 교환하는 거래를 주문하면 ETH/USD 유동성 풀의 구성은 25,000개의 ETH와 96,000,000개의 USD로 바뀌고 거래자는 4,000,000개의 USD를 받게 되며, 거래 전후 ETH와 USD의 수량의 곱은 2,400,000,000,000으로 동일하게 유지된다. Fig. 3은 위의 예시를 도식화한 것이다.

상수급 마켓 메이커는 용어의 사전적 의미 그대로 유동성 풀을 구성하는 두 자산의 수량의 곱을 일정하게 유지하는 것이 원칙이지만, 유동성 공급자에게 지분에 따라 거래 수수료를 분배하는 인센티브가 도입된 실제 거래 환경에서는 자산의 거래가 체결될 때마다 유동성 풀에 거래 수수료만큼 자산의 수량이 누적되어 두 자산의 수량의 곱이 조금씩 증가한다.

앞선 예시와 동일하게 ETH/USD 유동성 풀에 24,000개의 ETH와 100,000,000개의 USD가 공급되어 있고 어

떤 거래자가 1,000개의 ETH를 USDT로 교환하려 하는 경우, 거래 수수료가 0.3%라고 가정하면 1,000개의 ETH가 거래에 사용되기 이전에 0.3%에 해당하는 3개의 ETH가 먼저 유동성 풀에 누적되어 두 자산 ETH와 USDT 수량의 곱을 갱신하고(2,400,000,000,000에서 2,400,300,000,000으로 증가), 그 다음으로 나머지 997개의 ETH가 거래에 사용되어 3,988,000개의 USDT와 교환된다. 상수급 마켓 메이커를 사용하는 거래 플랫폼의 자산 교환 수량 계산식을 나타낸 Equation (1)에 0.3%의 거래 수수료를 반영하면 Equation (2)와 같다.

$$y = \beta - \{(\alpha + 0.003 \times x) \times \beta\} / (\alpha + x) \quad (2)$$

유동성 풀 내 자산 수량의 곱을 일정하게 유지하는 상수급 마켓 메이커가 탈중앙화 거래 시장에서 일반적으로 채택되는 이유는 이 마켓 메이커가 거래를 처리할 때 거래의 규모에 관계없이 거래에 사용되는 유동성 풀의 어느 한 자산의 유동성도 0보다 크게 유지된다는 장점 때문이다. 거래 페어 중 어느 한 쪽의 유동성이 고갈되지 않는다는 이러한 명확한 장점이 있지만 상수급 마켓 메이커를 포함하여 자동화 마켓 메이커를 사용하는 거래 플랫폼이 갖는 단점도 존재하는데, 거래의 효율, 즉 거래를 주문할 때 예상할 수 있는 결과가 거래에 사용되는 유동성 풀의 규모나 거래 자체의 규모에 따라 크게 달라질 수 있다는 점이다. 구체적으로는 거래 규모에 비해 유동성 풀의 규모가 작을수록, 그리고 유동성 풀의 규모에 비해 거래의 규모가 클수록 거래의 효율이 감소하고, 반대로 유동성 풀의 규모가 클수록, 그리고 거래의 규모가 작을수록 거래의 효율이 증가한다.

유동성 풀 규모의 차이가 비용 효율에 미치는 영향을 살펴 보기 위한 예를 들면, 만약 거래수수료 0.3%를 적용한 앞선 예시에서 ETH/USDT 유동성 풀의 유동성 규모가 24,000 ETH와 100,000,000 USDT의 50% 수준인 12,000 ETH와 50,000,000 USDT였다면, 1,000개의 ETH를 USDT로 교환할 때 얻을 수 있는 USDT는 약 3,834,615개로 약 3.8% 감소했을 것이고, 유동성 규모가 10% 수준인 2,400 ETH와 10,000,000 USDT 였다면 약 26.5% 감소한 약 2,932,353 개의 USDT만을 얻을 수 있었을 것이다.

거래 규모의 차이가 비용 효율에 미치는 영향을 살펴보기 위한 예를 들면, 만약 유동성 풀의 규모가 24,000 ETH와 100,000,000 USDT인 ETH/USDT 유동성 풀에서 기존 예시인 1,000 ETH의 2배에 해당하는 2,000 ETH를 USDT로 교환할 경우 약 7,669,231 USDT를, 10배에 해당하는 10,000 ETH를 USDT로 교환할 경우 약 29,323,529 USDT를 얻을 수 있을 것이다. 자산의 거래 규모가 클수록 더 많은 자산으로 교환되는 것은 자명하지만 교환 비율은 각각 3,834.6155

USDT/ETH와 2,932.3529 USDT/ETH로 기존 예시의 경우인 3,988 USDT/ETH에 비해 각각 약 3.8%, 26.5% 감소함을 알 수 있다.

3.2 단일 거래 경로 라우팅 알고리즘

이전 장의 예시에서 확인할 수 있는 것처럼 자동화 마켓 메이커를 사용하는 거래 환경에서 거래의 비용 효율은 유동성 풀의 규모와 거래의 규모에 따라 달라지며, 경우에 따라서는 거래 효율의 변동폭이 커지기도 한다. 이는 하나의 거래에 대해 하나의 유동성 풀을 사용하는, 이를테면 ETH와 USDT 간의 거래에 대해 ETH/USDT 유동성 풀 하나만을 사용하는 경우에 흔히 볼 수 있는 현상인데, 이를 개선하기 위한 방법으로 필요에 따라 다른 유동성 풀을 사용하도록 거래 경로를 우회, 즉 변경하여 거래의 비용 효율을 개선하는 거래 경로 라우팅 알고리즘이 도입되기 시작하였고, 가장 먼저 자동화 마켓 메이커를 채택했던 유니스왑에서 서로 다른 유동성 풀을 조합하여 거래 경로를 구성할 수 있도록 하는 라우터(Router) 컨트랙트를 업데이트하여 처음으로 이를 구현하였다.

거래 경로 라우팅 알고리즘이 거래의 비용 효율을 개선하는 유효한 방법이 되는 근본적인 배경은 자동화 마켓 메이커를 채택한 거래 플랫폼은 그 거래 환경의 특성상 많은 수의 유동성 풀이 존재한다는 점에 있다. 예를 들어 ETH를 USDT로 교환하고자 하는 경우 ETH/USDT 유동성 풀을 사용하는 것이 일반적이지만, 만약 해당 거래 플랫폼에 ETH/USDC 유동성 풀과 USDC/USDT 유동성 풀이 구성되어 있다면 경우에 따라서는 ETH/USDC 유동성 풀을 통해 ETH를 먼저 USDC로 교환한 뒤 USDC/USDT 유동성 풀을 통해 USDC를 USDT로 교환하는 것이 거래의 효율이 더 높을 수 있다. 이전 장의 예시를 통해 24,000개의 ETH와 100,000,000개의 USDT로 구성된 ETH/USDT 유동성 풀에서 1,000개의 ETH를 USDT로 교환할 경우 거래 수수료 0.3%를 고려하면 3,988,000개의 USDT로 교환할 수 있음을 살펴보았는데, 만약 해당 예시에서 ETH/USDT 유동성 풀 이외에 48,000개의 ETH와 200,000,000개의 USDC로 구성된 ETH/USDC 유동성 풀과 300,000,000개의 USDC와 300,000,000개의 USDT로 구성된 USDC/USDT 유동성 풀이 함께 존재하고 있었을 경우, 1,000개의 ETH를 ETH/USDT 유동성 풀을 통해 USDT로 교환하는 대신 ETH/USDC 유동성 풀과 USDC/USDT 유동성 풀을 각각 거쳐 USDT로 교환했다면 약 4,002,882개의 USDT로 교환할 수 있었을 것이다. 유동성 풀을 2번 거치는 만큼 거래수수료도 2회 지불하게 되지만 그럼에도 불구하고 거래의 비용 효율이 더 높을 수 있는 이유는 ETH → USDC → USDT 거래 경로에서 사용하는 ETH/USDC 및 USDC/USDT 유동성 풀의 유동성 규모가 기존의 ETH → USDT 거래 경로에서 사용한 ETH/USDT

유동성 풀의 유동성 규모보다 충분히 크기 때문이다.

주목할 만한 점은 위의 예시처럼 거래 경로를 구성하는 각 유동성 풀의 유동성 규모가 충분히 클 경우, 거래가 체결되기 이전에 각 유동성 풀을 구성하던 자산의 비율을 통해 계산할 수 있는 거래 경로의 유동성 비율이 다른 거래 경로에 비해 더 낮더라도 거래의 효율이 더 높을 수 있다는 점이다. 예를 들어 ETH → USDC → USDT 거래 경로를 사용한 위의 예시에서 ETH/USDC 유동성 풀을 구성하는 ETH의 수량이 48,000개가 아니라 48,050개였다면, ETH/USDC 유동성 풀과 USDC/USDT 유동성 풀의 각 자산 수량으로 계산한 ETH → USDC → USDT 거래 경로의 유동성 비율은 약 4162.3309 USDT/ETH로 기존의 ETH → USDT 거래 경로의 유동성 비율인 약 4166.6667 USDT/ETH보다 불리해지게 되지만, 실제로 거래를 수행할 경우 1,000개의 ETH로 교환할 수 있는 USDT 수량이 약 3,998,856개로 기존의 ETH → USDT 거래 경로보다 여전히 거래의 효율이 더 높게 된다.

이전의 예시들에서 확인할 수 있는 것처럼 자동화 마켓 메이커를 사용하는 거래 플랫폼에서 거래의 비용 효율에 영향을 주는 일차적인 요인은 유동성 풀의 규모와 거래의 규모이다. 하지만 실제로는 거래 수수료를 비롯하여 다양한 거래 경로와 여러 유동성 풀을 구성하는 각 자산의 비율과 같은 세부적인 요소들을 모두 고려해야 최적의 비용 효율을 얻을 수 있는 거래 경로를 도출할 수 있다. 또한 특정 시점에 거래 플랫폼에 존재하는 모든 유동성 풀에 대하여, 어떤 자산을 어떤 규모만큼 지불하여 어떤 자산으로 교환하고자 할 때 어떤 유동성 풀을 활용하여 거래 경로를 선택해야 최적의 효율을 얻을 수 있는지, 즉 거래를 통해 얻고자 하는 자산을 가장 많은 수량만큼 교환할 수 있는지 파악하기 위해서는 선택 가능한 거래 경로들을 모두 시뮬레이션 할 필요가 있다. 그러나 탈중앙화 거래 플랫폼에 존재하는 유동성 풀의 수는 일반적으로 수십, 경우에 따라서는 수백 개에 달하기 때문에 이들로 조합 가능한 거래 경로의 수많은 경우의 수를 모두 탐색하는 것은 비효율적이고 따라서 실제로는 몇 가지 제약사항을 두어 전체 경우의 수를 줄이는 것이 일반적이다. 예를 들어 유니스왑의 경우 유동성이 가장 높은 5개 자산인 이더리움(ETH), 랩트비트코인(WBTC), 유에스티테더(USDT), 유에스티코인(USDC), 다이(DAI)를 거래의 중간자(intermediary), 즉 거래 경로를 우회할 때 거쳐갈 수 있는 자산으로 사용하도록 지정하고 있고, 각 단일 거래 경로에서 사용할 수 있는 유동성 풀의 최대 수(max hop)를 3개까지로 제한하고 있다.

5가지 자산을 중간자로 지정하고 거래 경로를 구성하는 유동성 풀의 수를 최대 3개까지로 제한했기 때문에 유니스왑에서 자산이 거래될 때 고려 대상이 되는 거래 경로의 수는 최대 26개가 되고, 거래자가 제시한 주문에 대해 각 거래 경로의 비용 효율을 모두 계산한 뒤 가장 높은 효율을 얻을 수

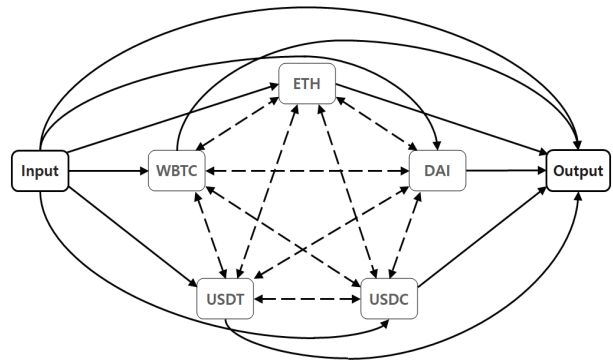


Fig. 4. Searching Transaction Path

있는 거래 경로를 도출하는 것이 유니스왑에서 도입한 거래 경로 라우팅 알고리즘의 구체적인 작동 방식이다. Fig. 4는 유니스왑에서 사용 가능한 거래 경로를 탐색하는 루트를 도식화한 것이다.

최초의 자동화 마켓 메이커 기반 탈중앙화 거래 플랫폼인 유니스왑에서 거래 경로 라우팅 알고리즘을 도입한 이후 많은 후발주자들이 이를 모방한 로직을 업데이트하는 것이 흔히 보이게 되었을 정도로 최적의 거래 경로를 찾는 방법에 대한 수요가 증가하였는데, 이러한 거래 경로 라우팅 알고리즘은 거래의 효율을 개선한다는 점에서 큰 의의를 가지며, 그 외에도 여러 유동성 풀을 활용하여 더 많은 유동성 공급자에게 거래 수수료 혜택을 제공할 수 있다는 측면에서의 장점도 생각해볼 수 있다. 유니스왑의 경우 가장 유동성이 풍부한 5개 자산을 거래의 중간자로 지정하였기 때문에, 해당 5개 자산으로 구성할 수 있는 총 10가지 유동성 풀에 대한 유동성 공급 수요를 확보할 수 있었을 것이다.

4. 다중 거래 경로 라우팅 알고리즘

본 장에서는 본 논문에서 제안하는 다중 거래 경로 라우팅 알고리즘의 아이디어와 구체적인 원리에 대해 설명한다. 본 장에서 알고리즘을 설명할 때 실제 교환 비율과 유동성 비율이라는 용어를 특히 많이 사용하는데, 유동성 비율은 3.2절에서 살펴본 것처럼 어떤 거래 경로를 구성하는 유동성 풀들의 자산 구성 비율에서 계산 가능한 이론상의 자산 교환비율, 실제 교환 비율은 실제로 거래가 수행된 이후에 그 결과로부터 계산되는 실제 자산 교환비를 의미한다.

4.1 제안 알고리즘의 개요

유니스왑을 시작으로 자동화 마켓 메이커를 채택한 많은 탈중앙화 거래 플랫폼에서 도입하기 시작하고 있는 거래 경로 라우팅 알고리즘은 필요에 따라 기존과 다른 거래 경로를 선택해 다양한 유동성 풀을 활용하여 거래의 비용 효율을 개

선하지만, 항상 단일 거래 경로만을 사용한다는 단점이 있다. 다시 말해서 기존의 거래 경로 라우팅 알고리즘은 거래의 규모에 관계없이 단일 거래 주문의 모든 거래량을 단일 거래 경로를 통해서만 소화한다. 이전 장에서 주요 예시로 들었던, 24,000 ETH와 100,000,000 USDT로 구성된 ETH/USDT 풀, 48,000 ETH와 200,000,000 USDC로 구성된 ETH/USDC 풀, 300,000,000 USDC와 300,000,000 USDT로 구성된 USDC/USDT 풀 등 세 종류의 유동성 풀이 있을 때 1,000개의 ETH를 USDT로 교환하고자 하는 예시의 경우 기존의 거래 경로 라우팅 알고리즘은 항상 ETH → USDC → USDT 경로를 최적의 거래 경로로 제시하고, 거래 수수료가 0.3%로 동일할 때 1,000개의 ETH는 항상 약 4,002,882개의 USDT로 교환되며, ETH/USDT 유동성 풀은 항상 사용되지 않는다.

본 논문에서 제안하는 다중 거래 경로 라우팅 알고리즘은 위의 예시에서 ETH/USDT 유동성 풀이 사용되지 않는다는 점에 착안하였다. 기존의 거래 경로 라우팅 알고리즘에서 ETH/USDT 유동성 풀을 사용하는 거래 경로를 선택하지 않고 ETH/USDC 유동성 풀과 USDC/USDT 유동성 풀을 함께 사용하는 거래 경로를 선택하는 이유는 1,000개의 ETH를 거래에 사용하는 같은 거래 규모에 대해 거래 수수료를 2회 지불하더라도 더 높은 비용 효율을 얻을 수 있을 정도로 두 유동성 풀의 유동성 규모가 충분히 크기 때문이었다. 해당 예시에서 거래 수행 이전에 계산 가능한 각 거래 경로의 유동성 비율은 두 경로 모두 약 4166.6667 USDT/ETH이고, 거래 수행 이후에 계산 가능한 ETH → USDC → USDT 경로의 실제 교환 비율은 약 4002.882 USDT/ETH인데, 해당 거래에서 사용되지 않은 거래 경로(ETH → USDT)의 유동성 비율과 해당 거래에서 사용된 거래 경로의 실제 교환 비율의 차이가 클 수록 더 많은 거래 효율 개선의 여지가 남아있게 된다는 것이 본 논문에서 제안하는 알고리즘의 핵심 아이디어이다.

위 예시에서 만약 ETH → USDC → USDT 경로의 거래에 사용된 거래량의 일부를 ETH → USDT 경로에 할당한다고 가정하면, ETH → USDC → USDT 경로의 경우 거래 규모가 감소하기 때문에 실제 교환 비율, 즉 거래의 효율이 증가하게 되고, 반대로 ETH → USDT 경로의 경우 기존의 유동성 비율보다 작은 실제 교환 비율 값을 가지게 되며 이 경로에 할당되는 거래량이 많을 수록 실제 교환 비율, 즉 거래의 효율이 감소하게 된다. 예를 들어 위의 예시에서 전체 거래 규모인 1,000 ETH의 55%인 550 ETH 만큼만 기존 경로인 ETH → USDC → USDT 경로를 통해 거래하고 나머지 45%에 해당하는 450 ETH는 ETH → USDT 경로를 통해 거래하면 ETH → USDC → USDT 경로를 통해 약 2,235,300개의 USDT를, ETH → USDT 경로를 통해 약

Table 1. Trade Ratio and Result of each path

Split Ratio	Path 1 Trade Ratio	Path 2 Trade Ratio	Result
0 %	4002.8820 USDT/ETH		4,002,882 USDT
10 %	4004.0161 USDT/ETH	4127.3901 USDT/ETH	4,016,353 USDT
20 %	4020.1613 USDT/ETH	4113.1747 USDT/ETH	4,038,764 USDT
30 %	4036.4372 USDT/ETH	4099.0569 USDT/ETH	4,055,223 USDT
40 %	4052.8455 USDT/ETH	4085.0356 USDT/ETH	4,068,793 USDT
45 %	4064.1818 USDT/ETH	4077.7089 USDT/ETH	4,070,269 USDT
50 %	4069.3878 USDT/ETH	4071.1100 USDT/ETH	4,070,249 USDT

1,834,969개의 USDT를 교환하여 총 약 4,070,269개의 USDT를 교환할 수 있는데, 이 경우 기존 단일 거래 경로(ETH → USDC → USDT)의 실제 교환 비율(4002.882 USDT/ETH)보다 높은 유동성 비율(4166.6667 USDT/ETH)을 갖는 거래 경로(ETH → USDT)에 거래 규모의 일부를 할당한 결과 기존 경로의 실제 교환 비율이 약 4002.882 USDT/ETH에서 약 4064.1818 USDT/ETH로 상승하고, 새로 선택된 추가 경로(ETH → USDT)의 실제 교환 비율은 기존의 유동성 비율이었던 약 4166.6667 USDT/ETH에서 약 4077.7089 USDT/ETH로 감소하여 두 경로 간의 교환 비율 차이가 줄어드는 것을 알 수 있다. Table 1은 거래 규모를 나눠 처리하기 전후를 비교한 위의 예시와 추가 예시를 정리한 것이다.

위의 예시와 표를 통해 알 수 있는 것처럼, 기존의 단일 거래 경로의 실제 교환 비율보다 높은 유동성 비율을 갖는 추가 거래 경로에 거래량의 일부분을 할당하면 전체 거래의 비용 효율을 더욱 개선할 수 있다. 이 때 추가 경로에 할당되는 거래량이 증가함에 따라 전체 거래의 비용 효율이 증가하다가 어느 시점부터 감소하게 되는데, 그 시점의 거래의 비용 효율이 해당 추가 거래 경로를 선택했을 때에 개선시킬 수 있는 비용 효율의 상한선이 된다. 예를 들어 ETH → USDC → USDT 경로에 더하여 ETH → USDT 경로를 추가 경로로 사용하는 위의 예시에서 전체 거래량의 50%만큼을 추가 경로인 ETH → USDT 경로에 할당하여 거래할 경우, ETH → USDC → USDT 경로를 통해 약 2,035,555개의 USDT를, ETH → USDT 경로를 통해 약 2,034,694개의 USDT를 교환하여 총 약 4,070,249개의 USDT를 교환할 수 있는데, 이는 추가 경로에 거래량의 40%만큼을 할당했던 표의 예시의 결과인 약 4,068,793 USDT 보다는 증가한 수치이지만, 45%만큼을 할당했던 예시의 결과인 약 4,070,269 USDT 보다는 감소한 수치이므로, 추가 경로에 거래량을 할당하는 비율을 기준으로 40%와 50% 사이 어딘가에 거래의 비용 효율의 증감 추세가 반전되는 지점이 있음을 알 수 있다.

이러한 관점에 착안하여 거래의 비용 효율의 증가 추세가 반전되기 시작하는 지점의 거래량 분배 비율을 이후에 설명

할 알고리즘에 따라 소수점 둘째 자리까지 계산하면 47.43%가 되는데, 즉 전체 거래 규모인 1,000 ETH 중 525.7 ETH를 기존 경로로, 나머지 474.3 ETH를 추가 경로로 거래를 진행하여 약 4,070,446 USDT로 교환하는 것이 주어진 환경(ETH/USDT, ETH/USDC, USDC/USDT 유동성 풀)에서 1,000 ETH를 USDT로 교환하는 더 좋은 방법이 된다.

4.2 제안 알고리즘의 소개

본 논문에서 제안하는, 자동화 마켓 메이커를 사용하는 거래 환경에서 사용 가능한 다중 거래 경로 라우팅 알고리즘의 원리는 간단한데, 기존의 거래 경로 라우팅 알고리즘에서 사용되는 최적의 단일 경로를 도출하는 메커니즘을 응용하여 차선의 추가 경로를 탐색하는 것이다. 즉 단일 거래 경로 사용을 가정했을 때의 최선의 거래 경로를 먼저 도출한 뒤, 해당 거래 경로를 제외하고 선택 가능한 나머지 거래 경로들 중에서 다시 한 번 최선의 거래 경로를 계산하여 차선의 거래 경로를 탐색한다.

차선의 거래 경로를 탐색한다 하더라도 주어진 거래 조건에서 조합 가능한 모든 거래 경로에서 최적 단일 경로 하나만을 제외한 나머지 거래 경로들을 모두 고려하는 것은 비효율적일 수 있다. 최적 단일 거래 경로를 탐색할 때는 가능한 모든 거래 경로를 시뮬레이션하게 되지만, 일단 최적 단일 거래 경로가 확정된 뒤에는 해당 거래 경로의 실제 교환 비율을 기준으로 하여 나머지 거래 경로들 중 이 교환 비율보다 유리한 유동성 비율을 갖는 거래 경로만을 선출하여 추가 거래 경로의 후보 경로로 고려하면 연산 시간을 줄일 수 있다.

이러한 방식으로 두 번째 거래 경로로 선택 가능한 후보 경로를 선별한 뒤, 각 후보 경로를 두 번째 거래 경로로 선택했다고 가정할 경우에 대하여 4.1절의 예시와 같이 가장 높은 거래 효율을 얻을 수 있는 거래 결과를 시뮬레이션하고, 각 후보 경로에 대하여 그 값이 가장 높은 경로를 두 번째 거래 경로로 선택한다. 이 시뮬레이션 과정에서 최적 단일 거래 경로, 즉 첫 번째 거래 경로의 거래량을 추가 경로에 얼마나 배분해야 가장 높은 거래 효율을 얻을 수 있는지 계산하게 되는데, 본 논문에서 제안하는 다중 거래 경로 라우팅 알고리즘에서는 전체 탐색 방법(Brute-Force Method)을 사용하여 이를 구현하였다.

두 번째 거래 경로를 탐색하는 과정과 같은 방식으로 세 번째와 네 번째 등 추가 거래 경로를 탐색할 수 있는데, 전체 탐색 방법을 사용하여 동시에 여러 경로에 거래량을 배분하는 경우의 수를 탐색하는 알고리즘의 특성상 동시에 탐색하는 경로의 수에 따라 전체 연산 규모가 기하급수적으로 증가한다는 단점이 있다. 따라서 본 논문에서 제안한 다중 거래 경로 라우팅 알고리즘에서는 주어진 거래 조건에 대하여 최대 3개의 경로를 동시에 사용하는 거래 경로를 탐색하되, 각

Algorithm 1 Multi-Path Routing Algorithm (Dual Path)

Input: input asset A , input amount x , output asset B

Output: optimized paths p_s, p_d , split ratio r_{p_s}, r_{p_d}

```

1: Build available path list  $P$ 
2:  $y_{p_{max}} = 0$ 
3: for each path  $p$  in  $P$  do
4:    $y_p = T(A, x, B, p)$ 
5:   if  $y_p > y_{p_{max}}$  then
6:      $p_{max} = p, y_{p_{max}} = y_p$ 
7:   end if
8: end for
9:  $p_s \leftarrow p_{max}$ 
10: Build candidate path list  $C$ 
11:  $y_{c_{max}} = y_{p_{max}}$ 
12: for each path  $c$  in  $C$  do
13:    $y_{prev} = 0$ 
14:   for  $r = 0.001 \rightarrow 1$  do
15:      $y_{cur} = T(A, (1-r)x, B, p_s) + T(A, rx, B, c)$ 
16:     if  $y_{cur} > y_{prev}$  then
17:        $y_{prev} = y_{cur}$ 
18:     else
19:       break
20:     end if
21:   end for
22:   if  $y_{prev} > y_{c_{max}}$  then
23:      $c_{max} = c, y_{c_{max}} = y_{prev}, r_{c_{max}} = r - 0.001$ 
24:   end if
25: end for
26: if  $y_{c_{max}} == y_{p_{max}}$  then
27:    $c_{max} = ' ', r_{c_{max}} = 0$ 
28: end if
29:  $p_d \leftarrow c_{max}$ 
30:  $r_{p_s} \leftarrow 1 - r_{c_{max}}$ 
31:  $r_{p_d} \leftarrow r_{c_{max}}$ 
32: return  $p_s, p_d, r_{p_s}, r_{p_d}$ 

```

Fig. 5. Pseudocode of Algorithm Considering Dual Path

경로에 대한 거래 규모의 분배율을 결정할 때 백분율 기준 소수점 첫째 자리까지 고려하여 최적의 거래 경로를 제안하도록 하였다. Fig. 5는 두 번째 거래 경로까지 고려하는 경우의 알고리즘 의사코드이다.

5. 실험 및 분석

본 장에서는 본 논문에서 제안한 다중 거래 경로 라우팅 알고리즘을 평가하기 위한 실험을 설계하고 결과를 분석한다.

5.1 실험 설계

본 논문에서 제안하는 다중 거래 경로 라우팅 알고리즘의

성능을 평가하기 위한 비교 기준으로는 기존의 자동화 마켓 메이커 기반 탈중앙화 거래 플랫폼에서 사용되는 단일 거래 경로 라우팅 알고리즘을 사용한 거래 환경을 설정하였다. 무작위로 생성한 다수의 거래들로 구성된 대규모 거래량을 모두 처리할 때 다중 거래 경로 라우팅 알고리즘이 기존의 단일 거래 경로 라우팅 알고리즘보다 얼마나 거래의 효율을 높일 수 있는지 비교하여 평가를 진행하였는데, 다중 거래 경로 라우팅 알고리즘의 경우 동시에 2개의 거래 경로를 사용하는 이중 경로 라우팅 거래 환경과 3개의 거래 경로를 사용하는 삼중 경로 라우팅 거래 환경을 각각 가정하여 기존의 단일 경로 라우팅 거래 환경까지 총 세 가지 거래 환경을 가정하여 시뮬레이션을 수행하였다.

실제 탈중앙화 금융 시장에서는 주기적으로 체인링크[12]와 같은 오라클 서비스에 고가의 사용료를 지불하여 각 자산에 대해 가격 정보를 비롯한 양질의 데이터를 공급받아 이를 기준 데이터로 활용하거나, 거래가 진행됨에 따라 수시로 변하는 각 유동성 풀의 유동성 비율 데이터로부터 계산 가능한 각 자산의 '거래 플랫폼 상의 가격'을 사용하는 것이 일반적이다. 본 실험의 시뮬레이션 환경에서는 별도의 오라클을 사용하는 것이 불가하여 유동성 풀 데이터로부터 계산한 '거래 플랫폼 상의 가격'을 각 자산의 가격 데이터로 대신 사용하였으며, 각 거래 환경의 시뮬레이션 과정에서 거래 규모에 따라 거래에 사용되는 자산의 수량을 계산하는 것에 해당 가격 데이터를 활용하였다. 또한 성능 평가 기준으로 시뮬레이션 과정에서 각 거래 환경별 거래 처리 후에 각 자산 수량의 차이를 고려하였는데, 예를 들어 어떤 자산을 ETH로 교환하고자 하는 거래의 경우 단일 거래 경로, 이중 거래 경로, 삼중 거래 경로를 고려하는 각 거래 환경에서 각각 교환 가능한 ETH 수량의 차이를 비교하였으며, 해당 데이터를 바탕으로 모든 거래가 수행된 이후 기존의 단일 거래 경로 라우팅 알고리즘 대비 다중 거래 경로 라우팅 알고리즘의 거래 효율 우위를 백분율로 수치화한 데이터를 산출하여 비교하였다.

시뮬레이션 환경으로는 특정 시기의 실제 유니스왑 유동성 풀 데이터를 기준으로 0.3%의 거래 수수료를 적용하였으며, 거래에 사용되는 자산은 유니스왑에서 거래의 중간자로 지정하고 있는 5개 자산인 이더리움(ETH), 웹트비트코인(WBTC), 유에스디테더(USDT), 유에스디코인(USDC), 다이(DAI)로 한정하였다. 유동성 풀 데이터는 2021년 상반기에 유니스왑이 가장 높은 TVL을 형성하던 시기인 5월 초, 이더리움 1242만 번째 블록이 생성된 시점의 유동성 풀 데이터를 사용하였으며, 해당 유동성 풀 데이터는 Table 2와 같다.

각 시뮬레이션에서 전체 거래 규모는 \$100,000,000으로 설정하였으며, 사전에 지정된 최소 및 최대 거래 규모 범위 내에서 개별 거래의 거래 규모가 무작위로 선택되도록 하여 평균 거래 규모가 특정 값으로 수렴되도록 유도하였다. 거래

Table 2. Liquidity Pool Data

Liquidity Pool	Liquidity
USDC / ETH	176,543,532.779424 USDC / 41,092.5244954087 ETH
ETH / USDT	41,757.4709065028 ETH / 180,162,827.16507 USDT
WBTC / ETH	2,942.21948724 WBTC / 39,304.8563813923 ETH
DAI / ETH	85,016,363.900768104 DAI / 19,773.0719684517 ETH
USDC / USDT	31,349,099.329648 USDC / 31,451,658.201203 USDT
DAI / USDC	8,884,478.5793577185 DAI / 8,874,379.23313 USDC
DAI / USDT	7,942,486.5582593766 DAI / 7,946,278.329379 USDT
WBTC / USDC	38.59889702 WBTC / 2,202,104.229854 USDC
WBTC / DAI	11.43788286 WBTC / 653,369.4224214992 DAI
WBTC / USDT	0.24136994 WBTC / 13,589.399021 USDT

에 사용되는 자산인 입력 자산과 거래 후 받는 자산인 출력 자산 또한 각 거래별로 무작위로 지정되며, 각 거래가 수행되는 시점의 유동성 풀 데이터로부터 계산되는 자산 가격을 기준으로 해당 거래에 사용되는 입력 자산의 수량이 계산되도록 하였다. 거래 수수료는 고려되었지만, 실제 블록체인 환경에서 블록에 트랜잭션이 포함되는 순서의 차이로 인해 발생할 수 있는 슬리피지(slippage)나 트랜잭션 작성 시 지불하게 되는 가스비는 고려되지 않았다.

본 논문에서는 각 유동성 풀의 유동성 규모와 전체 거래 규모가 동일할 때 각 개별 거래의 평균 거래 규모에 따라 다중 거래 경로 라우팅 알고리즘의 거래 효율 개선 정도가 어떻게 달라지는지 확인하기 위해 평균 거래 규모가 각각 \$5,000, \$15,000, \$25,000, \$75,000, \$125,000이 되도록 무작위 거래를 생성하여 시뮬레이션을 진행하였으며, 각 평균 거래 규모에 대하여 \$100,000,000 규모의 전체 거래를 처리하는 시뮬레이션을 10회씩 진행한 뒤 그 평균값을 계산하여 정리하였다.

5.2 결과 분석

1) 평균 거래 규모에 따른 거래 효율 개선도

Fig. 6은 평균 거래 규모별로 기존의 단일 거래 경로 라우팅 알고리즘 대비 다중 거래 경로 라우팅 알고리즘의 거래 효율 개선 정도를 백분율로 나타낸 것으로, 거래가 시작되는 시점의 유동성 규모가 같을 때 각 거래의 평균 거래 규모가 클수록 최대 2개 경로의 동시 사용을 고려하는 이중 경로 라우팅 환경과 최대 3개 경로의 동시 사용을 고려하는 삼중 경로 라우팅 환경 간의 거래 효율 개선 정도의 차이가 벌어지는 것을 확인할 수 있다. 구체적으로는 평균 거래 규모가 \$5,000일 때 이중 경로 라우팅 환경 대비 삼중 경로 라우팅 환경의 거래 효율 개선도의 차이가 약 11% 수준이었던 반

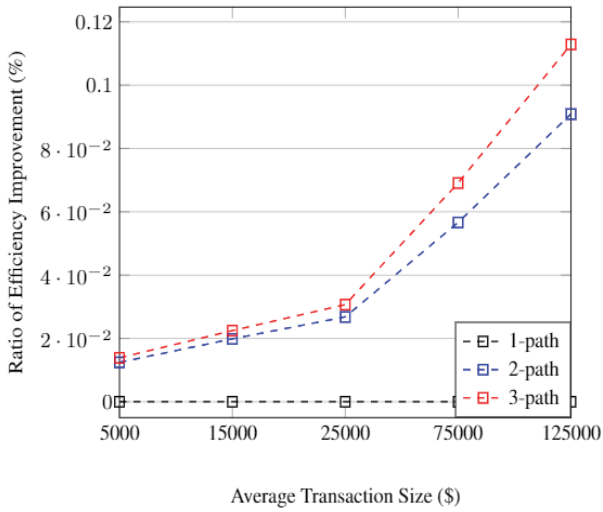


Fig. 6. Ratio of Efficiency Improvement by Average Transaction Size

면, 평균 거래 규모가 \$125,000일 때는 이 차이가 약 24% 수준으로 증가하였다. 이러한 결과가 나타나는 이유는 전체 거래 규모가 같다고 하더라도 이를 구성하는 각 개별 거래의 거래 규모가 클수록 기존의 단일 경로를 사용하는 방식보다 동시에 여러 경로를 사용하여 거래 규모를 분산시켜 처리하는 것이 거래의 효율을 끌어올릴 수 있기 때문이다.

2) 평균 거래 규모에 따른 실제 동시 사용 경로 수의 비율

본 논문에서 제안한 알고리즘의 아이디어 검증 단계에서 확인된 것은, 동시에 여러 개의 경로를 사용하는 것을 고려 하더라도 경우에 따라서는 동시에 1개의 경로를, 즉 단일 경로를 사용하는 것이 최선의 거래 효율을 낼 수 있다는 것이

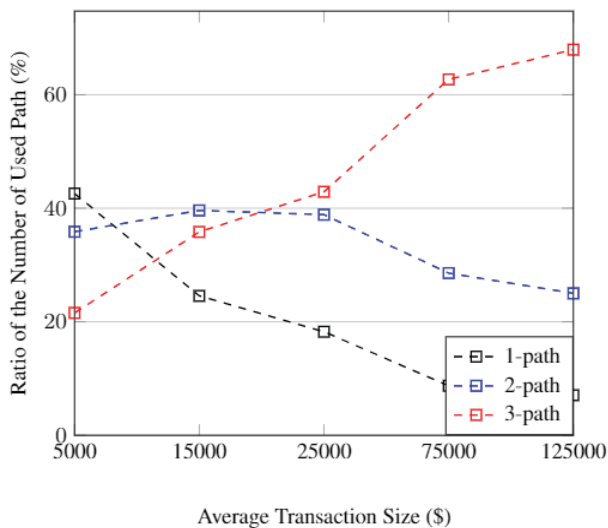


Fig. 7. Ratio of the Number of Used Path by Average Transaction Size

다. 동시에 다수의 경로를 사용하는 것을 고려하는 이유는 기존의 단일 경로를 거쳤을 경우에, 두 자산 간의 교환 비율 보다 더 높은 유동성 비율을 갖는 다른 경로가 있다면 해당 경로를 통해 거래 규모의 일부를 동시에 처리하는 것이 전체 거래 효율을 높일 수 있기 때문이었는데, 경우에 따라서는 이러한 조건을 만족하는 다른 경로가 없을 수도 있으며, 이 경우 기존의 방법대로 단일 경로를 사용하는 것이 최선의 거래 효율을 내는 선택지가 된다.

Fig. 7은 평균 거래 규모에 따른 거래 효율 개선도를 확인 하기 위한 앞 장의 시뮬레이션을 진행하는 과정에서, 각 개별 거래 수행 시 동시에 몇 개의 경로를 사용하여 거래를 처리하는 것이 최선의 선택이었는지 그 비율의 변화를 정리한 것이다. 예를 들어 평균 거래 규모가 \$5,000이었을 경우 전체 거래 규모를 구성하는 각 개별 거래의 43%는 단일 거래 경로를, 36%는 이중 거래 경로를, 나머지 21%는 삼중 거래 경로를 사용하여 거래를 처리하는 것이 최선의 선택이었으며, 평균 거래 규모가 \$125,000일 때는 이 비율이 단일 거래 경로의 경우 7%, 이중 거래 경로의 경우 25%까지 감소하였고 삼중 거래 경로의 경우 75%까지 증가하였다. 이를 통해 개별 거래의 평균 거래 규모가 작을수록 동시에 탐색하는 경로의 수가 적은 것이 유리한 경우가 많고, 평균 거래 규모가 클수록 이 수가 많은 것이 유리한 경우가 많다는 것을 확인할 수 있다.

3) 유동성 규모에 따른 거래 효율 개선도

Fig. 8은 전체 거래 규모 \$100,000,000을 구성하는 개별 거래의 평균 거래 규모가 \$25,000인 경우에 대한 시뮬레이션을 진행하는 과정에서 계산된 각 자산별 평균 거래 효율 개선도를 나타낸 것으로, 예를 들어 어떤 자산을 USDT로 교환

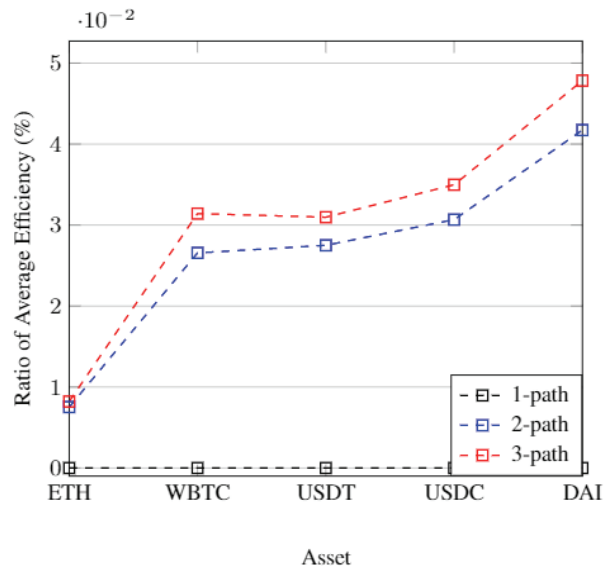


Fig. 8. Ratio of Average Efficiency by Asset

하고자 하는 거래의 경우 기존의 단일 거래 경로 라우팅 알고리즘 대비 다중 거래 경로 라우팅 알고리즘의 거래 효율 개선도는 이중 거래 경로를 고려할 때 약 0.0275%, 삼중 거래 경로를 고려할 때 약 0.0310%이다. 주목할 만한 것은 기존 알고리즘 대비 다중 거래 경로 라우팅 알고리즘의 거래 효율 개선도가 ETH의 경우 평균 약 0.0079%로 USDT의 경우보다 낮았고, 반면 DAI의 경우 평균 약 0.0448%로 더 높았다는 점인데, 이는 전체 유동성 풀을 구성하는 각 자산 별 유동성의 규모의 차이로 인한 것으로 보인다. 다시 말해서 ETH의 경우 USDT보다 자산의 유동성의 크기가 크기 때문에 일반적으로 거래 효율 개선도가 더 낮았고, DAI의 경우 USDT보다 자산의 유동성의 크기가 작기 때문에 거래 효율 개선도가 더 높았다고 볼 수 있으며, 이는 전체 거래 규모와 이를 구성하는 개별 거래의 평균 거래 규모가 같을 때 유동성 규모에 따라 다중 거래 경로 라우팅 알고리즘의 거래 효율 개선도가 달라질 수 있다는 것을 의미하는 것으로 분석할 수 있다.

6. 결론 및 향후 연구

블록체인 기술을 사용하는 탈중앙화 분산 금융 시장이 등장하고 이 기술을 사용하는 암호화폐의 글로벌 자산시장 내 지분이 증가함에 따라 분산 금융 시장에 많은 자본 유동성이 유입되면서 분산 금융 시장에 적용할 수 있는 여러 알고리즘이나 이 시장의 기반이 되는 블록체인 플랫폼 자체에 대한 기술적인 연구가 많아지고 있다. 본 논문에서는 탈중앙화 거래 시장에서 가장 일반적으로 채택되고 있는 자동화 마켓 메이커 기반 거래 플랫폼에 적용 가능한 다중 거래 경로 라우팅 알고리즘을 제안하였으며, 실험을 통해 해당 알고리즘이 기존에 쓰이던 단일 거래 경로 라우팅 알고리즘에 비해 거래의 비용 효율을 개선할 수 있음을 보였다. 그러나 본 논문에서는 다중 거래 경로를 탐색하는 과정에서 전체 탐색 기법을 사용하였으며, 블록체인 플랫폼에서 각 트랜잭션마다 발생하는 가스비를 고려하지 않았기 때문에 한계점이 존재한다. 따라서 향후 연구를 통해 다수의 거래 경로를 탐색하기 위한 추가 탐색 기법의 조사와 함께 각 블록체인 플랫폼마다 상이한 트랜잭션 가스비를 고려한 실험을 진행할 필요가 있다.

References

[1] G. Angeris, H. T. Kao, R. Chiang, C. Noyes, and T. Chitra, "An analysis of Uniswap markets," *arXiv preprint arXiv:1911.03380*, 2019.

[2] W. Warren and A. Bandeau, "0x: An open protocol for decentralized exchange on the Ethereum blockchain," [Internet], <https://github.com/0xProject/whitepaper> (downloaded 2021, Aug. 1).

[3] J. Xu, K. Paruch, S. Cousaert, and Y. Feng, "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols," *arXiv preprint arXiv:2103.12732*, 2021.

[4] M. Bartoletti, J. H. Chiang, and A. Lluch-Lafuente, "A theory of Automated Market Makers in DeFi," In *International Conference on Coordination Languages and Models* (pp. 168-187). Springer, Cham, 2021.

[5] DefiLlama [Internet], <https://defillama.com>.

[6] H. Adams, N. Zinsmeister, and D. Robinson, "Uniswap v2 Core," [Internet], <https://docs.uniswap.org/whitepaper.pdf> (downloaded 2021, Aug. 10).

[7] Vitalik Buterin, Let's run on-chain decentralized exchanges the way we run prediction markets [Internet], https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way.

[8] A. Capponi and R. Jia, "The adoption of blockchain-based decentralized exchanges: A market microstructure analysis of the automated market maker," Available at SSRN 3805095, 2021.

[9] G. Angeris and T. Chitra, "Improved price oracles: Constant function market makers," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pp.80-91, 2020.

[10] V. Mohan, "Automated market makers and decentralized exchanges: A defi primer," Available at SSRN 3722714, 2020.

[11] Wrapped Tokens: A multi-institutional framework for tokenizing any asset [Internet], <https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf>.

[12] L. Breidenbach et al., "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks," [Internet], <https://research.chain.link/whitepaper-v2.pdf> (downloaded 2021, Oct. 1).



정 현 빈

<https://orcid.org/0000-0002-5962-0058>
 e-mail : jhbin194@gmail.com
 2020년 서강대학교 컴퓨터공학과(학사)
 2022년 서강대학교 컴퓨터공학과(석사)
 관심분야 : 블록체인, 탈중앙화 금융



박 수 용

<https://orcid.org/0000-0002-3979-0586>

e-mail : sypark@ccs.sogang.ac.kr

1986년 서강대학교 컴퓨터공학과(학사)

1988년 Florida State University,
Computer and Information
Science(석사)

1995년 George Mason University, Information Technology
(박사)

현 재 서강대학교 컴퓨터공학과 교수 및 지능형블록체인센터
센터장

관심분야: 소프트웨어공학, 블록체인