코스모스 기반 AMM 기능 제안

Lite Paper

변동삼, 이형연

2021-02

Contents

1 버전

버전	날짜	작성자	내용
0.1	2021-02-03	변동삼 이형연	피어 리뷰 목적

2 개요

최근 블록체인 기술의 발달로 개발자들은 무신뢰 (trustless) 환경에서 작동 가능한, 확장 가능하고 자동화된 어플리케이션을 구현할 수 있게 되었다. 그중 가장 중요한 발전을 이룬 것이 바로 AMM(자동시장조성) 기능이다 (“Uniswap V2 Core” 2020). 이를 통해 투자자들은 상당한 자본이나 금융공학에 대한 이해 없이도 시장조성 활동에 참여할 수 있게 되었다.

코스모스 네트워크 (“What Is Cosmos?” 2021) 의 경우 IBC(Inter-Blockchain Communication; 블록체인 간 통신 프로토콜)(“Cosmos IBC” 2021) 라는 중요한 기술적 진보를 달성한 바 있다. IBC 기술은 코스모스 기반 블록체인들 사이에 토큰이 편리하게 오갈 수 있도록 할 뿐만 아니라, IBC Peg 라는 기술을 통해 한 블록체인에서 토큰을 예금하고 다른 블록체인에서 출금하는 것도 가능케 한다. 예를 들어 ETH Peggy(“Cosmos ETH Peggy” 2021) 와 BTC Peg 를 통해 사용자들은 이더리움 혹은 비트코인 자산을 코스모스 네트워크로 끌어올 수도 있다.

이러한 기술적 발전을 바탕으로 이 문서에서는 코스모스 생태계를 위한 탈중앙거래소 (DeX) 를 제안한다. 이 DeX 모듈은 기존의 호가형 거래 시스템, AMM(Automated Market Making), 그리고 일괄 체결 방식을 결합하여 코스모스 허브에 높은 유동성을 제공할 것이다. 또한 IBC 와 Peg 기능을 바탕으로 코스모스 생태계 내에서 많은 토큰 거래 수요가 발생할 것이므로, DeX 를 주축으로 한 시장이 허브 내 핵심 유틸리티로 자리잡을 것이다.

3 Uniswap AMM 기반 모델

근래 이더리움 생태계에선 탈중앙금융 (DeFi) 시장이 눈에 띄게 발전하였으며, 대표적인 선두주자로 Uniswap 의 AMM 모델 ("Uniswap V2 Core" 2020) 이 있다.

AMM 이란 주어진 알고리즘을 바탕으로 사용자들이 토큰을 교환할 수 있는 일종의 DeX 메커니즘이다. AMM 은 다음과 같은 여러 가지 이점을 제공한다:

- 시장조성의 민주화: 상당한 자본이나 금융공학 기술이 없어도 누구나 AMM 유동성 풀 (liquidity pool) 에 토큰을 입금함으로써 시장조성에 참여할 수 있다.
- 중개자 제거: AMM 은 분산형 블록체인 네트워크를 기반으로 구축된다. 이를 통해 사용자는 중앙화된 운영자 또는 자금의 신탁 없이 다양한 금융활동을 할 수 있다.
- 토큰 교환의 단순화: 사용자는 복잡한 호가창에 의존하지 않고도 토큰 교환을 할 수 있다.

AMM 은 크게 복잡하지 않으면서도 시장에 많은 이로움을 가져다주었고 변화하는 시장 환경 속에서도 안정성을 보여주었다 (Angeris et al. 2020). 하지만 이러한 AMM 방식에도 단점이 있는데, 주문 체결 우선수위와 가격 비일관성의 문제가 있다.

3.1 가격 비일관성

AMM 모델의 핵심은 **곱불변 방정식**이다. 곱불변 방정식이란 토큰 x 와 토큰 y 그리고 양의 상수 k 에 대하여 $R_x R_y = k$ 가 성립함을 뜻하며, 여기서 R_x 와 R_y 는 각각 유동성 풀에 예치된 토큰 x 와 토큰 y 의 수량을 의미한다. 두 수량을 곱한 k 의 값은 토큰 교환 전 (t) 과 후 (t+1) 에도 일정하게 유지된다:

$$R_x(t)R_y(t) = R_x(t+1)R_y(t+1) \tag{3.1}$$

만약 사용자가 Δ_x 만큼의 토큰을 교환할 경우, 곱 $R_x R_y$ 는 다음과 같이 바뀐다.

$$\begin{aligned} R_x(t)R_y(t) &= R_x(t+1)R_y(t+1) \\ &= \left(R_x(t) + \Delta_x\right)\left(R_y(t) - \Delta_y\right) \\ &= \left(R_x(t) + \Delta_x\right)\left(R_y(t) - \frac{\Delta_x}{p_s}\right) \end{aligned} \tag{3.2}$$

이때 $p_s = \Delta_x / \Delta_y$ 는 토큰 교환 가격이다.

우변을 전개하고 식을 정리하면

$$\begin{aligned} R_x(t)R_y(t) &= R_x(t)R_y(t) - R_x(t)\frac{\Delta_x}{p_s} + \Delta_x R_y(t) - \frac{\Delta_x^2}{p_s} \\ &\Rightarrow \frac{\Delta_x(R_x(t)+\Delta_x)}{p_s} = \Delta_x R_y(t) \\ &\Rightarrow \frac{R_x(t)+\Delta_x}{p_s} = R_y(t) \\ &\Rightarrow p_s = \frac{R_x(t)+\Delta_x}{R_y(t)} \end{aligned} \tag{3.3}$$

마지막으로 $\Delta_x = cR_x(t)\ (0 < c < 1)$ 을 대입하면 다음의 식을 얻는다.

$$\begin{aligned} p_s &= \frac{R_x(t)+\Delta_x}{R_y(t)} \\ &= \frac{R_x(t)+cR_x(t)}{R_y(t)} \\ &= (1+c)\frac{R_x(t)}{R_y(t)} \\ &= (1+c)p_p(t) \end{aligned} \tag{3.4}$$

이때 $p_p(t) = R_x(t)/R_y(t)$ 는 토큰 교환 전 풀 가격이다.

한편, 토큰 교환 후 풀 가격은 다음과 같다.

$$\begin{aligned} p_p(t+1) &= \frac{R_x(t+1)}{R_y(t+1)} \\ &= \frac{R_x(t)+\Delta_x}{R_y(t)-\Delta_y} \\ &= p_s + \frac{\Delta_x}{R_y(t)} + \frac{\Delta_x^2}{R_x(t)R_y(t)} \\ &= (1+c)^2 p_p(t) \end{aligned} \tag{3.5}$$

여기서 주목할 점은 토큰 교환 후 풀 가격이 토큰 교환 가격보다 $(1+c)$ 배만큼 크다는 것이다. 이러한 가격 비일관성은 몇 가지 문제를 야기한다:

- 토큰 교환 가격과 풀 가격의 불일치로 인해 풀 가격이 필요 이상으로 등락하여 과도한 차익거래가 유발된다
- 불필요하게 많은 차익거래는 유동성 풀 투자자 및 거래자들의 추가적인 손실로 이어질 수 있다

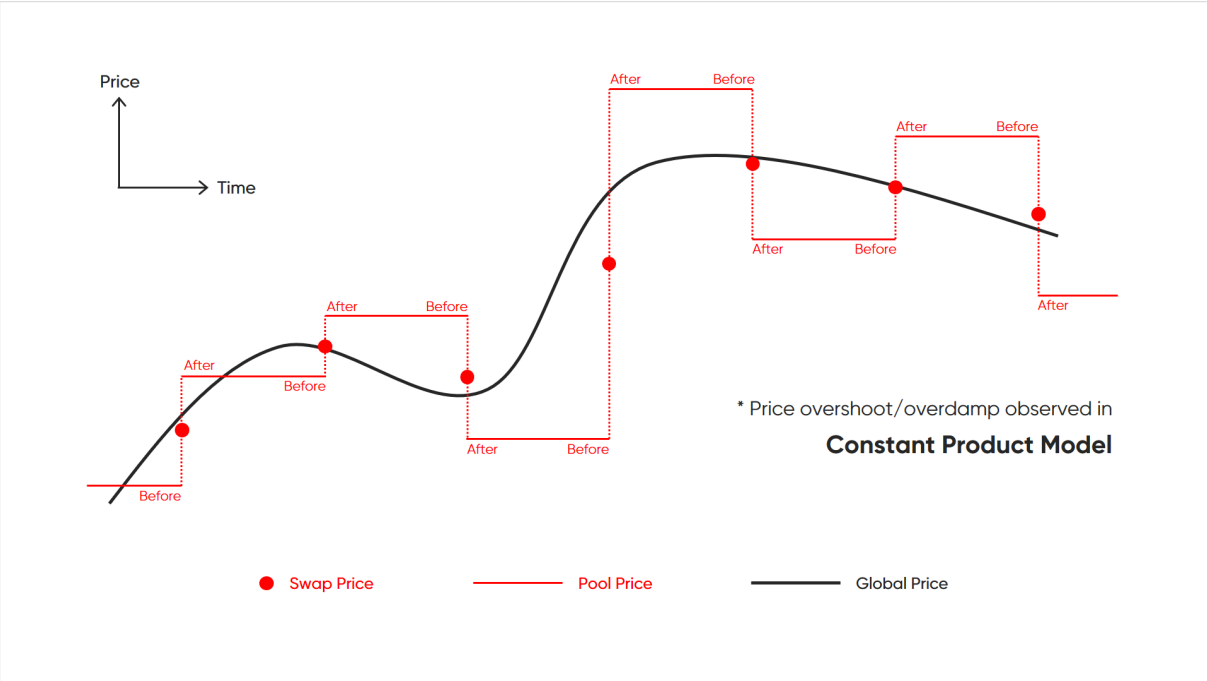

Figure 3.1: 곱불변 모델에서의 비효율적인 가격 발견

3.2 주문 체결 우선순위

유니스왑이 기반으로 하는 이더리움의 경우, 블록 채굴자들은 블록 내 트랜잭션 처리 순서를 마음대로 결정할 수 있으며 이러한 처리 순서의 변동은 Uniswap 에서 각 주문의 체결 가격에 큰 영향을 미친다. 이는 비단 PoW(작업증명) 네트워크뿐만 아니라 PoS(지분증명) 및 dPoS(위임지분증명) 네트워크 환경에서도 발생한다 (Zhou et al. 2020). 특히 앞서 언급한 가격 비일관성의 문제와 결합되면 거래자는 상당히 불리한 조건으로 거래하게 될 수도 있다.

트랜잭션 우선순위 조정의 두 번째 문제는 지연성 (latency) 및 가스 (gas) 경쟁이다. 거래자들은 자신의 주문을 우선적으로 체결시키기 위해 경쟁하게 되므로 가스 가격이 올라가게 된다. 또한 채굴자와 거래자 간의 공모를 통한 선행 매매 (front running)의 문제를 야기할 수 있다.

3.3 주문 유형

현재 Uniswap AMM 모델에선 주문을 넣는 즉시 결과가 성공 또는 실패로 확정되기 때문에 주문이 블록 한 개를 넘어 존재할 수 없다. 즉 이번 블록에 들어온 모든 주문은 즉시 체결되거나 전부 소멸되며, 이 과정에서 유동성이 함께 소실되므로 새로운 주문을 반복적으로 넣어줘야 한다.

또한, 기존 AMM 메커니즘은 기본적으로 지정가 주문을 허용하지 않는다. 지정가 주문이란 토큰 매매 시 원하는 가격을 지정하여 제출하는 주문을 말한다. 지정가로 제출된 주문은 체결될 때까지 오더북 (orderbook; 호가창) 에 남아있거나 주문자의 요청으

로 취소될 수 있다. 이는 시장가 주문과 달리 사용자가 원하는 가격에서 주문이 체결될 수 있도록 하므로 더 효율적인 가격 발견과 더욱 적극적인 시장 참여 활동을 장려한다. 거래자들이 다양한 전략을 구사할 수 있게 됨으로써 시장의 유동성이 늘어나고 이는 토큰 교환 시 발생하는 슬리피지 (slippage) 를 줄여주므로 거래 비용을 낮추는 효과가 있다.

3.4 부분 체결

물량이 큰 주문은 일시에 체결되기가 어렵기 때문에 여러 거래자들과 서로 다른 가격으로 작은 주문들을 통해 체결될 수 있다. 이 과정에서 거래자들은 더 합리적인 가격을 찾을 수 있고 높은 수준의 유동성이 유지될 수 있다. 하지만 이러한 부분 체결 방식은 기존 AMM 모델에선 적용이 불가능한 시스템이다.

4 코스모스 AMM 모델 제안

위의 연구를 토대로, 전통적인 오더북 기반 시스템 (“Traditional Orderbook System” 2021) 과 AMM 방식을 결합한 하이브리드 모델을 제안한다.

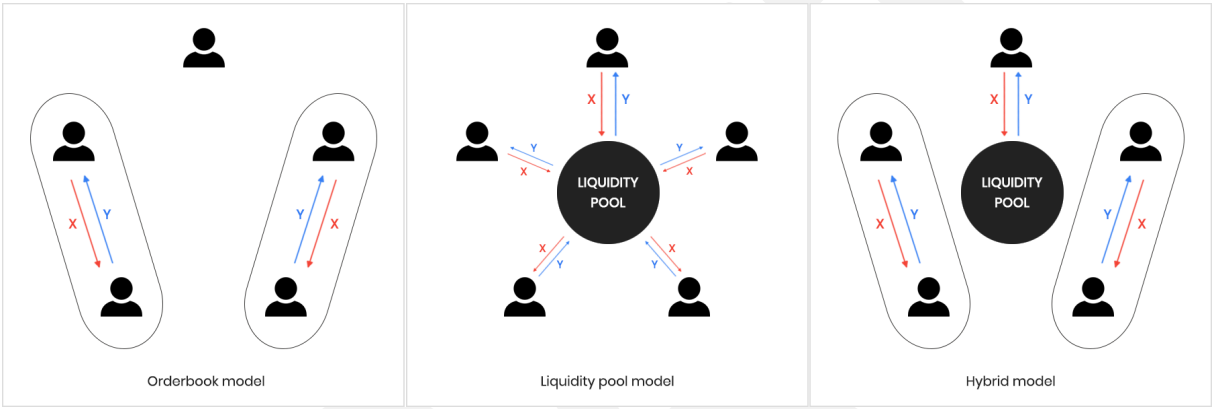

Figure 4.1: 세 가지 유형의 토큰 교환 모델

- 모든 주문은 오더북에 누적된다
- 일괄 체결 (batch execution) 이 진행되는 블록 높이에서 주문 매칭 엔진을 통해 오더북상 주문들이 체결된다
- 유동성 풀은 4.3절에서 소개될 동일교환가격 모델에 따라 주문 매칭에 참여한다

또한 해당 모델에선

- 지정가 주문을 허용하며 해당 주문이 체결되거나 주문자에 의해 취소될 때까지 오더북에 머무를 수 있다
- 주문 가격이 해당 시점의 토큰 교환 가격과 동일할 경우 부분 체결을 허용한다

4.1 일괄 체결

체결 우선순위 문제를 해결하기 위해 해당 모델에선 **일괄 체결 (Batch Execution)** 방식을 제안한다. 이는 (Pourpouneh, Nielsen, and Ross 2020) 에서 제안된 “일괄 경매 *(batch auction)*” 맥락에서 착안한 것이다.

> 대안적인 해결책은 연속적인 *(continuous)* 체결이 아닌 개별적인 *(discrete)* 체결 과정을 활용하는 "일괄경매" 방식의 탈중앙거래소이다. 짧은 주기로 반복되는 일괄 경매 방식은 주문이 처리되는 속도의 불확실성을 제거하여 모든 매수자와 매도자가 동등한 거래 기회를 가지도록 한다. 원하는 가격을 선점하기 위해 주문 순서에 매달릴 필요 없이, 주어진 시간 동안 누구나 원하는 가격에 원하는 만큼 주문을 넣을 수 있다. 이러한 일괄경매 방식은 전통 금융시장에서 초단타매매 *(High Frequency Trading)* 에 의해 발생하는 선행매매 문제를 해결하기 위해 고안되었다 *(Budish et al. 2014).* 암호화폐 시장에 있어서도 일괄 경매 방식은 많은 여러 문제를 해결할 수 있으며 특히 모든 매수, 매도 주문이 동등하게 처리되기 때문에 선행매매 문제가 직접적으로 해결된다. 주문이 많을 경우 일괄 처리하는 시간 범위를 조정함으로써 성능 문제 또한 해결할 수 있다.

제출된 주문은 유동성 풀에 모여 정해진 시간 동안 머물다가 일괄 체결 과정을 통해 체결되며 처리되지 않은 주문은 오더북에 남는다.

하이브리드 모델은 크게 두 가지 특징을 지닌다:

- 체결되지 않은 주문은 오더북에 머물며 향후 일괄배치를 대기한다
- 일괄 체결 주기는 시장 상황에 따라 변할 수 있다. 예를 들어 새로운 주문이 대거 유입되어 토큰 교환 가격이 크게 변동할 경우 일괄 체결 주기가 길어질 수 있다. 일괄 체결 주기가 길어지면 더 많은 거래자들이 가격 발견에 참여할 수 있게 되어 더 균형있고 안정적인 거래가 가능해진다. 이는 여러 온라인 경매 플랫폼에서 사용되는 "유동적 경매마감 (dynamic closing)" 혹은 "연장 입찰 (extended bidding)" 모델과 유사하다 ("Auction Terminology" 2020).

(Pourpouneh, Nielsen, and Ross 2020) 이 언급하였듯, 일괄 체결 시스템이 적용된 탈중앙거래소는 선행 매매를 방지하고 채굴자/검증자 (validator) 와 거래자 간의 공모를 예방함으로써 보다 공평한 거래 환경을 조성할 수 있다.

4.2 주문 매칭 규칙

주문 매칭 모델은 아래 기준에 따라 부분 또는 전량 체결을 처리한다:

- 토큰 X 를 토큰 Y 로 교환 시
  - 주문 가격 > 교환 가격: 주문은 전량 체결된다
  - 주문 가격 = 교환 가격: 주문은 부분 또는 전량 체결된다
  - 주문 가격 < 교환 가격: 주문은 일절 체결되지 않는다
- 토큰 Y 를 토큰 X 로 교환 시
  - 주문 가격 < 교환 가격: 주문은 전량 체결된다
  - 주문 가격 = 교환 가격: 주문은 부분 또는 전량 체결된다
  - 주문 가격 > 교환 가격: 주문은 일절 체결되지 않는다

유동성 풀은 동일교환가격 모델에 기반하여 주문 매칭 과정에 유동성을 공급한다.

4.3 동일교환가격 모델

3.1에서 보았듯 곱불변 모델에선 토큰 교환 이후 풀 가격과 교환 가격이 달라지는 문제가 발생한다. 이로 인해 오더북 시스템과 유동성 풀 모델을 결합할 때에도 어려움이 생기는데, 주문 체결 후 오더북이 제시하는 가격과 유동성 풀이 제시하는 교환 가격이 서로 달라지기 때문이다. 이를 해결하고자 토큰 교환 가격과 교환 후 풀 가격이 같아지도록 계산식을 보정하였다:

$$p_s = p_p(t+1) = \frac{R_x(t) + \Delta_x}{R_y(t) - \Delta_x / p_s} \tag{4.1}$$

위의 식을 교환 가격 p_s 에 대하여 풀면 다음과 같다.

$$\begin{aligned} & p_s(R_y(t) - \Delta_x/p_s) = R_x(t) + \Delta_x \\ \Rightarrow \quad & p_s R_y(t) - \Delta_x = R_x(t) + \Delta_x \\ \Rightarrow \quad & p_s = \frac{R_x(t) + 2\Delta_x}{R_y(t)} \end{aligned} \tag{4.2}$$

마지막으로 $\Delta_x = cR_x(t)\ (0 < c < 1)$ 을 대입하면 다음의 식을 얻는다.

$$\begin{aligned} p_s = p_p(t+1) &= \frac{R_x(t) + 2cR_x(t)}{R_y(t)} \\ &= (1+2c)\frac{R_x(t)}{R_y(t)} \\ &= (1+2c)p_p(t) \end{aligned} \tag{4.3}$$

이 모델에선 최근 교환 가격이 풀 가격과 완전히 일치하기 때문에 곱불변 모델에 비하여 차익 거래 기회가 줄어든다.

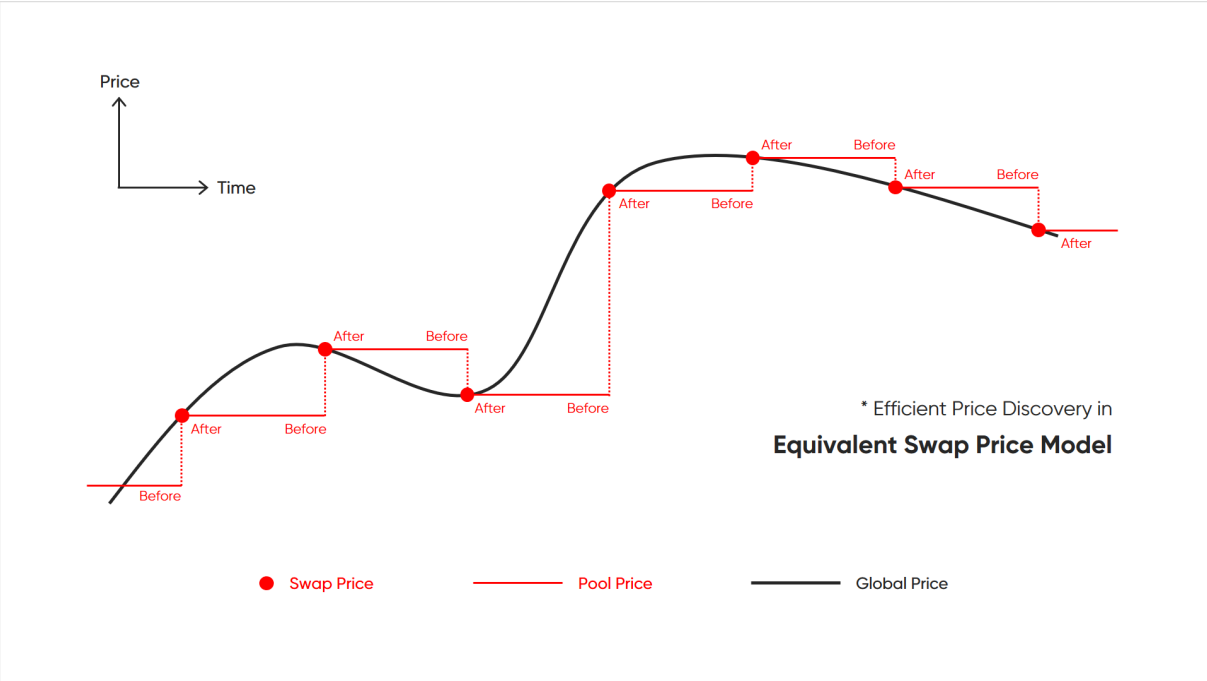

Figure 4.2: 동일교환가격 모델에서의 효율적인 가격 발견

여기서 주목할 점은 두 가격을 일치시킴으로써 곱불변 방정식이 성립하지 않는다는 점이다. 즉 유동성 풀에 담긴 토큰의 갯수가 경로에 의존적임을 의미한다. (Buterin 2017)

이 모델은 주어진 교환 가격 p_s 에 대하여 유동성 풀이 처리하는 주문 수량을 다음과 같이 계산한다.

$$\begin{aligned} \Delta_x &= \Delta_y = 0 && (p_s = p_p) \\ \Delta_x &= \frac{R_x - p_s R_y}{2} && (p_s < p_p) \\ \Delta_y &= \frac{p_s R_y - R_x}{2p_s} && (p_s > p_p) \end{aligned} \tag{4.4}$$

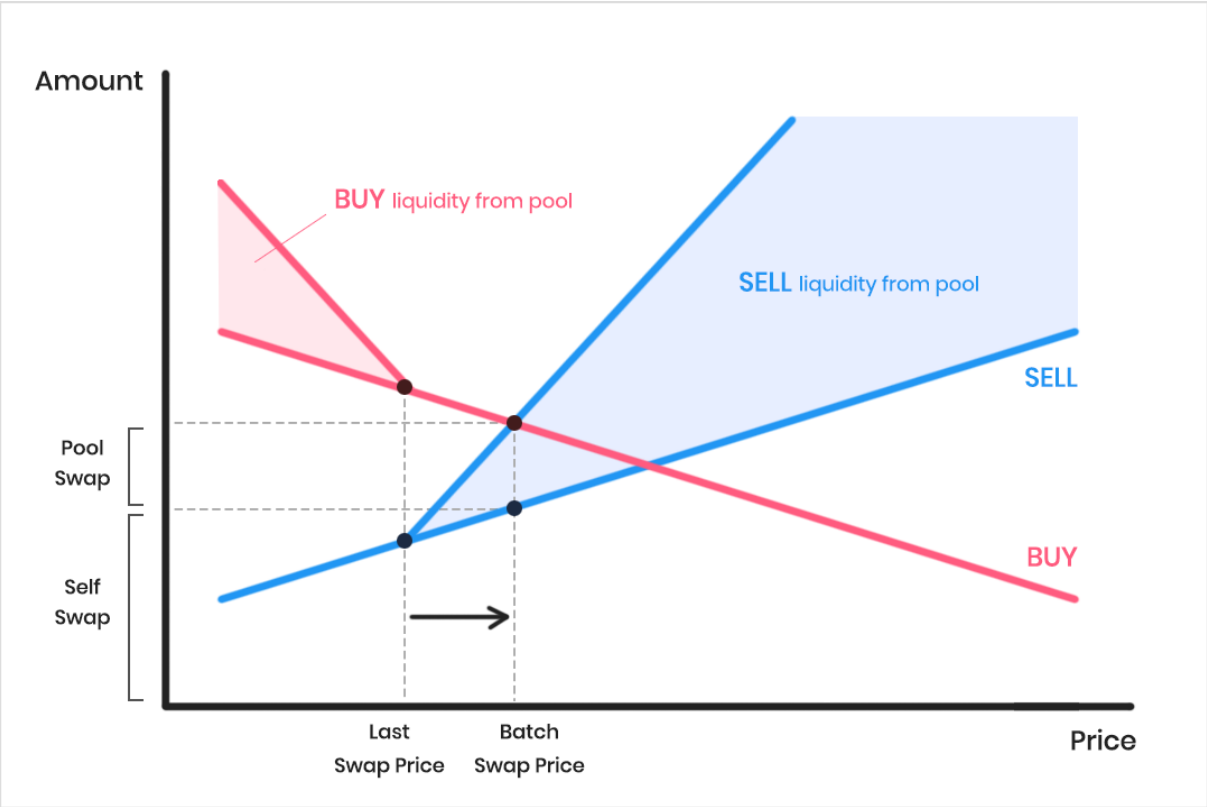

Figure 4.3: 수요와 공급

4.4 수수료

유동성 모듈은 크게 두 종류의 수수료를 포함하는데, 하나는 유동성 풀의 운영과 관련된 것이고 하나는 트랜잭션과 관련된 것이다. 각 수수료는 특정한 경제적 목적을 가지고 있다.

유동성 풀 운영 관련 수수료:

- **신규 풀 생성 수수료**: 새로운 유동성 풀을 생성할 때 수수료가 발생한다. 이는 풀이 과도하게 생성되는 것을 방지하고 기존에 존재하는 유동성 풀의 활용을 권장하기 위함이다. 풀 생성 수수료는 ATOM 으로 지불되며 Community Fund 에 적립된다.
- **풀 출금 수수료**: 유동성 풀에 투자한 자금을 출금할 때 출금액에 비례하여 수수료가 발생한다. 이 수수료는 출금한 풀에 다시 적립되며, 잦은 입출금을 바탕으로 한 취약점 공격으로부터 다른 풀 투자자들을 보호하기 위함이다.

트랜잭션 수수료

네트워크에 제출되는 모든 트랜잭션은 기본적으로 가스 (Gas) 수수료를 지불한다. 이 수수료는

- 블록 확정 시점에 지불된다

- 최종적으로 트랜잭션이 실패하더라도 지불된다
- ATOM 위임자, 검증자, 그리고 Community Fund 에게 배분된다 (“Gas and Fees” 2021)

또한, 교환된 토큰 수량에 비례하여 **토큰 교환 수수료**가 유동성 풀에 지불된다. 이 수수료는 풀에 누적되며 풀 투자자들의 투자액에 비례하여 각자에게 배분된다. 이는 Uniswap 모델과 유사하다.

초기 수수료율은 아래와 같이 제안한다:

- 토큰 교환 수수료율 = 0.003 (0.3%)
- 풀 출금 수수료율 = 0.003 (0.3%)
- 신규 풀 생성 수수료 = 100 ATOM

5 결론

본 제안서를 통해 코스모스 허브 AMM 의 기술적 디자인에 대해 살펴보았다. 우리는 이 유동성 모듈이 다음과 같은 특징을 바탕으로 코스모스 네트워크에 큰 경제적 효용을 안겨줄 것이라 생각한다:

- 중앙화된 운영자에 의존하지 않으면서 토큰 교환에 필요한 유동성을 공급한다
- 전통적인 오더북 기반 시스템과 AMM 방식을 결합함으로써 양질의 유동성을 제공한다
- 코스모스 네트워크 사용자들은 유동성 풀에 투자함으로써 수수료를 통한 수익 기회를 가질 수 있다
- (여러 DeFi 투자 토큰을 포함한) 어떤 종류의 토큰화된 자산이든 거래가 가능해진다

코스모스 허브 AMM 이 갖는 잠재력과 활용성은 무궁무진하며, 특히 IBC 를 통한 블록체인 간 자산 전송 기능과의 시너지를 통해 코스모스 허브가 블록체인 금융 생태계의 중심부로 자리매김할 수 있는 발판을 마련할 것이다.

모듈 구현과 관련된 세부 내용은 https://github.com/tendermint/liquidity/tree/develop 에서 확인할 수 있다.

참고문헌

Angeris, Guillermo, Hsien-Tang Kao, Rei Chiang, Charlie Noyes, and Tarun Chitra. 2020. “An Analysis of Uniswap Markets.” https://arxiv.org/pdf/2009.14021.pdf.

“Auction Terminology.” 2020. Wikipedia. 2020. https://en.wikipedia.org/wiki/Auction#Terminology.

Buterin, Vitalik. 2017. “On Path Independence.” 2017. https://vitalik.ca/general/2017/06/22/marketmakers.html.

“Cosmos ETH Peggy.” 2021. Althea. 2021. https://blog.althea.net/gravity-bridge/.

“Cosmos IBC.” 2021. Cosmos. 2021. https://docs.cosmos.network/v0.40/ibc/overview.html.

“Gas and Fees.” 2021. Cosmos. 2021. https://github.com/cosmos/cosmos-sdk/blob/afda62174fe6531b2a40c595a4d9396c28e8b391/docs/basics/gas-fees.md.

Pourpouneh, Mohsen, Kurt Nielsen, and Omri Ross. 2020. “Automated Market Makers.” IFRO Working Paper 2020/08. University of Copenhagen, Department of Food; Resource Economics. https://EconPapers.repec.org/RePEc:foi:wpaper:2020_08.

“Traditional Orderbook System.” 2021. Wikipedia. 2021. https://en.wikipedia.org/wiki/Order_book.

“Uniswap V2 Core.” 2020. Uniswap. 2020. https://uniswap.org/whitepaper.pdf.

“What Is Cosmos?” 2021. Cosmos. 2021. https://cosmos.network/intro.

Zhou, Liyi, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. 2020. “High-Frequency Trading on Decentralized on-Chain Exchanges.” https://arxiv.org/pdf/2009.14021.pdf.