# AMM(Automated Market Maker)기반 DEX(Decentralized Exchange)의 설계 및 활용

2025-1 AJOU SOFTCON


이 름 염수인

지도교수 김기형 교수님

멘 토 김종현 (데이터랩스)


## 개발동기 및 목적

최근 탈중앙화 금융(DeFi)은 기존 중앙화 금융의 한계를 보완하며 빠르게 성장하고 있다. 2024년 기준 DeFi 시장의 총 예치 자산(TVL)은 약 1,340억 달러(한화 약 200조원)로, 전년 대비 두 배 이상 증가했다. 이 성장의 중심에는 유동성 공급과 가격 결정을 자동화하여 탈중앙화 환경에서 시장을 구현하는 핵심 기술인 AMM이 있다.

AMM은 전통적인 오더북 방식 대신, 수학적 알고리즘을 통해 가격을 자동 조정하고 거래를 실행하는 구조로, 스마트 컨트랙트를 기반으로 중개자 없이 신뢰 가능한 거래 환경을 제공한다. 다만, 기존 AMM은 비효율적인 유동성 분배, 슬리피지, 높은 가스비, 비영구적 손실 등 여러 기술적 한계를 지닌다.

본 프로젝트는 이를 개선한 최신 AMM 구조(Uniswap V3 기반 Concentrated Liquidity Model)를 구현하고, 단순 구현을 넘어 AMM의 구조적 강점을 실용적인 서비스로 연결하는 데 목적을 둔다.

## 주요 기술 배경

### 스마트 컨트랙트

스마트 컨트랙트는 블록체인 위에 배포되어 자동으로 실행되는 프로그램이다. 중앙 서버나 제3자의 개입 없이도 계약 조건을 코드로 정의하고, 조건이 충족되면 자동으로 실행되며, 수정이나 조작이 불가능하다. 특히 AMM 시스템은 거래, 유동성 공급, 수수료 분배 등 모든 핵심 로직이 스마트 컨트랙트로 작성되어 신뢰성과 투명성을 확보한다.

### 유동성 풀

AMM은 오더북 없이 자산을 자동 교환하는 구조로, 그 중심에는 두 자산을 예치하는 유동성 풀이 있다. 사용자는 유동성 공급자로 참여하여 자산을 예치하고 거래 수수료를 보상받으며, 예치된 자산 비율에 따라 가격이 자동 조정된다. 이를 통해 누구나 중개자 없이 24시간 거래가 가능하며, 시장 수요에 따라 가격이 자연스럽게 형성된다.

### 집중화된 유동성

기존 AMM은 전체 가격 범위에 유동성을 균등하게 분산하여, 실제 거래가 발생하지 않는 구간에도 유동성이 묶이는 비효율이 존재한다. 이를 개선하기 위해 Concentrated Liquidity 모델이 도입되었다. 이 구조는 유동성을 특정 가격 구간에 집중시킬 수 있으며,자산 활용도를 높이고 슬리피지를 줄이는 데 효과적이다.

이러한 구조에서 유동성 공급자에 의해 공급되는 유동성의 변화량 $\Delta L$은 현재 가격과 공급 가격 범위의 관계에 따라 다음과 같이 계산된다. 여기서 $\Delta x$,$\Delta y$는 공급자가 예치하는 두 자산의 양, $P$는 현재 가격, $P_{lower}$, $P_{upper}$는 유동성 공급 가격 범위를 의미한다.

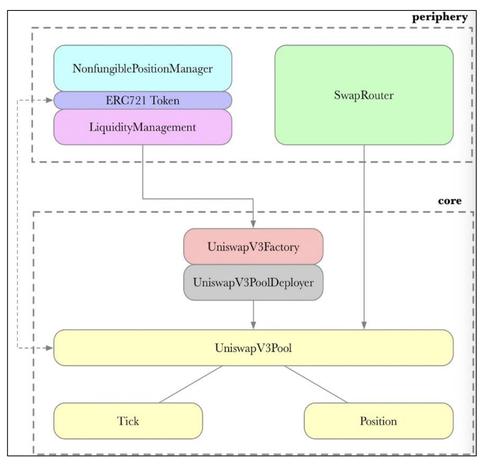
$$\Delta L = \begin{cases} \dfrac{\Delta y}{\sqrt{P_{\text{upper}}} - \sqrt{P_{\text{lower}}}} & P < P_{\text{lower}} \\ \min\left(\Delta x \cdot \dfrac{\sqrt{P_{\text{upper}}} \cdot \sqrt{P}}{\sqrt{P_{\text{upper}}} - \sqrt{P}}, \dfrac{\Delta y}{\sqrt{P} - \sqrt{P_{\text{lower}}}}\right) & P_{\text{lower}} \le P \le P_{\text{upper}} \\ \Delta x \cdot \dfrac{\sqrt{P_{\text{upper}}} \cdot \sqrt{P_{\text{lower}}}}{\sqrt{P_{\text{upper}}} - \sqrt{P_{\text{lower}}}} & P > P_{\text{upper}} \end{cases}$$

## 오픈소스 URL

https://github.com/vkdlqm369/myDex

## 개발 내용

### * 스마트 컨트랙트 구조




**NonfungiblePositionManager :** 유동성 공급자가 특정 가격 구간에 유동성을 공급/제거할 수 있도록 함. 각 포지션은 ERC-721(NFT)로 관리됨.

**SwapRouter** : 멀티홉 스왑을 고려한 최적의 스왑 경로를 라우팅하여 Pool을 호출함.

**Factory** : 두 자산 쌍과 수수료에 따라 고유한 Pool을 생성하여 배포함

**Pool** : 실제로 스왑과 유동성 공급, 수수료 계산 동의 로직이 실행되는 핵심 컨트랙트

### * Gas 최적화

스마트 컨트랙트는 P2P 환경에서 실행되며, 연산량에 비례한 가스(Gas) 비용이 발생해 사용자 수수료에 직접적인 영향을 미친다. 따라서 가스 최적화는 스마트 컨트랙트 구현에 있어 필수적인 요소이며, 이를 위해 다양한 최적화 기법을 적용한다.

#### 1. Tick

유동성 공급자가 유동성을 (0, ∞) 위의 임의의 실수 구간에 유동성을 공급할 수 있다면, 가격이 미세하게 변화하더라도 그에 따라 변화하는 유동성을 반영하기 위해서 많은 컴퓨팅 자원을 소모하게 된다. 따라서 가격 범위를 정해진 단위(Tick)로 이산적으로 분할하여 유동성을 관리한다. 가격 $P$를 Tick 인덱스 $i$에 따라 $p(i) = 1.0001^i$ 로 정의하여, 가격을 실수 대신 정수 인덱스로 관리함으로써 연산 효율을 확보하고 실수 연산에서 발생하는 오차를 줄일 수 있다.

#### 2. Liquidity Net (imos 법)

유동성을 $[i_{lower}, i_{upper}]$에 공급/제거하려면, 해당 범위의 모든 Tick을 순회하며 값을 갱신해야 하므로 연산 비용이 크다. 이를 해결하기 위해 Imos 법을 적용한다. 유동성 변화량을 구간의 시작과 끝 Tick에만 기록하고, 누적합을 통해 유동성 값을 효율적으로 계산한다.

#### 3. Initialized Bitmap

초기화되지 않은 Tick에 대한 불필요한 계산을 방지하기 위해, 각 Tick의 초기화 여부를 비트 마스킹하여 자료구조로 관리한다. 메모리 사용을 최소화하기 위해 이 구조는 (key, value) 형태의 Map으로 구현된다. 현재 Tick 인덱스를 $i$ 라고 하고 value의 size를 256bit라고 했을 때, Tick $i$ 의 초기화 여부는 $i/256$ 를 key로 갖는 value의 $i\%256$ 번째 비트로 표현된다.

## 활용방안 및 결론

본 프로젝트는 단순한 자산 거래를 넘어, AMM을 결제 시스템에 결합하는 새로운 활용 방안을 제시한다. Multi-hop Routing과 자동 환전 기능을 통해 실시간 최저가 결제가 가능하며, 중개자 없는 직접 거래로 수수료 부담도 최소화된다. 이는 기존 결제 시스템이 제공하지 못했던 유연하고 비용 효율적인 환경을 실현한다. 또한, 이 구조는 국가·통화·플랫폼을 초월한 보편적 결제 인프라로 확장될 수 있다. 그동안 디지털 자산 결제는 실질적 필요성과 효용이 부족하다는 평가를 받아왔으나, 본 프로젝트는 AMM의 강점을 결제에 접목함으로써 비용 절감, 자동화, 유연성을 갖춘 실질적 대안을 제시한다.