КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет комп'ютерних наук та кібернетики
Кафедра дослідження операцій

Знаходження найкращого шляху обміну у біржах на основі автоматизованих маркет-мейкерів

студента 4-го курсу
Байбули Кирила Аленовича

Київ — 2023

1 Реферат

Дана робота присвячена дослідженню методів обробки бірж основаних на методі автоматизованих маркет-мейкерів (з англ. "Automated Market Maker"). Головною метою роботи є розробка алгоритму знаходження найоптимальнішого шляху для динамічного графа, де вага ребра представляється у вигляді функцій від вкладів валют у конкретну пару в момент часу t та перевірка її оптимальності на існуючих системах що використов-ують AMM.

Умовні позначення

Позначення	Значення
AAM	Біржі основані на методі автоматичних маркет-майкерів.
X/Y	Пара на біржі валюти типу X та Y
$X \implies Y$	Короткий запис обміну валюти X на Y

2 Вступ

У світі фінансів і торгівлі цінними паперами, централізовані біржі завжди відігравали ключову роль, забезпечуючи місцезнаходження та централізовану інфраструктуру для трейдерів та інвесторів. Проте останнім часом відбувається зростання інтересу до децентралізованих бірж, що призводить до переворотних змін у фінансовому секторі. Децентралізовані біржі стають ключовим елементом цієї нової економічної парадигми. Підкріпленні математикою та детермінованими правилами, децентралізовані біржі забезпечують високу швидкість та надійність для їх користувачів та завдяки відкритості відкривають нові можливості для нових незалежних гравців ринку.

У данній роботі ми розглянемо біржі основані на методі автоматизованих маркет-мейкерів (з англ. "Automated Market Maker"). На відміну від традиційних бірж, де ціна визначається за допомогою зіставлення заявок купівлі та продажу, AAM використовують алгоритм для визначення ціни валюти, що залежить від кількості вкладів у валютну пару. Це дозволяє створити вигідну систему для владників ліквідності, що отримують винагороду за свої вклади, а також для бажаючих скористатися ліквідністю для обміну.

Також основною цілю нашого дослідженню буде біржа Uniswap V3 [1], котра є однією з найпопуляніших імплементацій AMM на даний момент.

2.1 Загальна математична модель

Нехай $G_t = (V_t, E_t)$ - неорієнтований динамічний граф, де V_t - множина вершин таких, що кожна вершина є конкретною валютою на біржі, E_t - множина ребер цього графа, тобто кожне ребро відображує те, чи є можливість на біржі обміняти деякі дві різні валюти з V_t, у момент часу t.

Так як в залежності від часу на біржі можуть з'являтися та зникати як валюти так і зв'язки (шляхи обміну) між ними, то ми описуємо біржу у вигляді динамічного графа, що залежить від часу t.

Також при обміні, має виконуватися таке рівняння:

$$x \cdot y = k = const \tag{1}$$

де x кількість валюти X, та y кількість валюти Y у парі X/Y, а k - деяка константа котра задається при створенні пари на біржі.

3 Формалізація графа

У даному розділі ми розширемо та формалізуємо модель описану у вступі (2.1).

3.1 Формула отримання кількості валюти в одній парі

Лема 1. *Нехай існує на біржі пара X/Y із об'ємом $a_{X/Y}$ вкладів валюти X та $b_{X/Y}$ вкладів валюти Y. Тоді об'єм у валюти Y при вкладанні x валюти X у пару X/Y дорівнює:*

$$y = \frac{b_{X/Y}x}{(a_{X/Y} + x)} \tag{2}$$

Доведення. Розглянувши (1) неважко вивести формулу отримуємої кількості y валюти Y при вкладанні x кількості валюти X у пару X/Y із вкладами a, b. Звідси з (1) до обміну відношення було:

$$a \cdot b = k$$

Після вкладу нової кількості x валюти в пару, отримуємо невідому кількість y з вкладу об'ємом b. При цьому по правилам протоколу відношення має залишатися незмінимим до і після обміну, тобто дорівнювати тому ж самому k, отже:

$$(a + x) \cdot (b - y) = k$$

Прирівнявши обидві рівності, отримаємо:

$$\begin{aligned} (a + x) \cdot (b - y) &= a \cdot b \\ (b - y) &= \frac{ab}{(a + x)} \\ (b - y) &= \frac{ab}{(a + x)} \\ y &= b - \frac{ab}{(a + x)} \end{aligned} \tag{3}$$

Або з (3) більш компактний варіант:

$$\begin{aligned} y &= \frac{ba + bx - ab}{(a + x)} \\ y &= \frac{bx}{(a + x)} \end{aligned} \tag{4}$$

■

3.2 Об'єм отримуємий при n-тій кількості переходів.

У кінцевій задачі ми будемо розглядати переходи між n-тою кількістю валют, тобто кількість переходів більше за $n > 2$, наприклад: $X \implies Y \implies Z$. Для цього спробуємо вивести її з (2).

Лема 2. *Нехай, a_i - об'єм вкладів пари **на котру** ми вносимо валюту C_i, а b_i - об'єм вкладів пари **з котрої** ми виносимо валюту C_{i+1} при i-тому обміні, де $i = \overline{0, n}$. Тоді об'єм обміну $C_0 \implies C_1 \ldots \implies C_{n-1} \implies C_n$ при вхідному x:*

$$y = x \prod_{i=1}^{n} b_i \div \left(\prod_{i=1}^{n} a_i + x \sum_{i=0}^{n-1} \left(\prod_{k=1}^{i} b_i \cdot \prod_{j=i+2}^{n} a_j \right) \right) \tag{5}$$

Ця формула достатня зручна, але при обрахуванні методами програмного забезпечення добутки вкладів можуть бути настільки великими числами (навіть два обміни між парами із вкладами по 10^6 утворює числа $(10^6)^3$), що при використанні чисел із обмеженою точністю може утворювати перевонення.

На момент написання цієї роботи, максимальний розмір регістра середньостатистичного комерційного комп'ютера скаладав 64 біта, де максимальне значення числа без знаку становить $2^{64} < 10^{20}$.

3.3 Визначення ваги ребра

Так як головною метою цієї роботи є опис загального алгоритму для знаходження найоптимальнішого шляху для обміну, ми спробуємо формалізувати визначення ваги у графі $G_t = (V_t, E_t)$.

Розглянувши формулу обміну (2) ми можемо побачити гіперболічну залежність вкладів однієї валюти від іншої.

Чим більшим ми вкладаємо валюти X тим більшим стає його відношення із Y, тим самим чим більше існує валюти X тим менш вона ціна відносно Y за мінімальну одиницю, тим самим AMM біржі балансують ціни.

Література

[1] Hayden Adams та ін. «Uniswap v3 core». В: *Tech. rep., Uniswap, Tech. Rep.* (2021).