НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 339.73

«До захисту допущено»
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптографічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Аналіз та обґрунтування властивостей DeFi моделі Constant Sum для вибору параметрів протоколу маржинальної торгівлі»**

Виконав:
студентка IV курсу, групи ФІ-93
Коваленко Дар'я Юріївна _____

Керівник:
доцент кафедри ММЗІ
ННФТІ НТУУ «КПІ ім.Ігоря Сікорського»,
д.т.н.,професор
Ковальчук Людмила Василівна _____

Рецензент:
доцент кафедри ІБ
ННФТІ НТУУ «КПІ ім.Ігоря Сікорського»
Барановський Олексій Миколайович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студентка _____

Київ — 2023

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Сергій ЯКОВЛЄВ
«__» _____ 2023 р.

ЗАВДАННЯ
на дипломну роботу

Студентка: Коваленко Дар'я Юріївна

1. Тема роботи: «*Аналіз та обґрунтування властивостей DeFi моделі Constant Sum для вибору параметрів протоколу маржинальної торгівлі*», науковий керівник дипломної роботи: доцент кафедри ММЗІ
ННФТІ НТУУ «КПІ ім.Ігоря Сікорського»,
д.т.н.,професор Ковальчук Людмила Василівна,
затверджені наказом по університету №__ від «__» _____ 2023 р.

2. Термін подання студентом роботи: «__» _____ 2023 р.

3. Об'єкт дослідження: *процес функціонування протоколу децентралізованих фінансів, що базується на моделі Constant Sum.*

4. Предмет дослідження: *вибір та обґрунтування максимально допустимого кредитного плеча та інших параметрів для моделі Constant Sum.*

5. Перелік завдань: *дослідження літератури щодо різних моделей функціонування децентралізованих фінансових протоколів; аналіз моделі Constant Sum; формулювання тверджень щодо властивостей цієї моделі та доведення цих тверджень; використання отриманих результатів для визначення параметрів функціонування цієї моделі та*

умови ліквідації; на базі отриманих результатів, обчислення можливих чисельних значень для допустимого плеча.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: *Презентація доповіді.*

7. Орієнтовний перелік публікацій: *планується доповідь на всеукраїнській конференції.*

8. Дата видачі завдання: 10 вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	01-15 вересня 2022 р.	Виконано
2	Опрацювання технічного матеріалу по темі дослідження	Вересень-жовтень 2022 р.	Виконано
3	Опис та дослідження процесу роботи моделі Constant Sum	Листопад - грудень 2022	Виконано
4	Доведення теорем про лінійність цієї моделі та про втрати при двох взаємно обернених свопах	Січень - лютий 2023	Виконано
5	Аналіз результатів числових експериментів для перевірки отриманих результатів. Проведення порівняння результатів з теоретичними підрахунками	Березень - квітень 2023	Виконано
6	Обгрунтування обмеження максимального допустимого кредитного плеча загальний та для окремого випадку	Травень - червень 2023	Виконано
7	Оформлення та захист дипломної роботи	Червень 2023	Виконано

Студент _____ Коваленко Д.Ю.

Керівник _____ Ковальчук Л.В.

РЕФЕРАТ

Кваліфікаційна робота містить: 51 стор., 7 рисунків, 12 джерел.

Дане дослідження було проведено з метою обгрунтування вибору параметрів протоколу маржинальної торгівлі.

Об'єктом дослідження є процес функціонування протоколу децентралізованих фінансів, що базується на моделі Constant Sum.

У ході роботи було проведено дослідження моделі Constant Sum. Проведена оцінка лінійності даної моделі. Здійснено розрахунки та аналіз результатів, щоб визначити, наскільки модель Constant Sum може бути лінійною та які фактори можуть впливати на її лінійність. Далі було визначено коефіцієнт взаємно обернених свопів, що є важливим показником для оцінки ризиків та стабільності протоколу маржинальної торгівлі. Окремо було розглянуто процес ліквідації позиції, який є важливою складовою протоколу маржинальної торгівлі та врешті-решт огрунтовано вибір максимального допустимого кредитного плеча.

Практичне значення результатів полягає в забезпеченні ефективного та стабільного функціонування протоколу маржинальної торгівлі. Вибір оптимального максимального кредитного плеча є важливим аспектом для забезпечення безпеки та уникнення ризиків для учасників ринку.

БЛОКЧЕЙН, ФІНАНСОВІ ПРОТОКОЛИ, ПРОТОКОЛ CONSTANT SUM, УМОВА ЛІКАВІДАЦІЇ, МАКСИМАЛЬНО ДОПУСТИМЕ КРЕДИТНЕ ПЛЕЧЕ

ABSTRACT

Qualification work contains: 51 pages, 7 figures, 12 sources.

This study was conducted to justify the choice of parameters of the margin trading protocol.

The object of research is the process of functioning of the decentralized finance protocol based on the Constant Sum model.

In the course of the work, the Constant Sum model was studied. The linearity of this model is estimated. The results were calculated and analyzed to determine the extent to which the Constant Sum model can be linear and what factors can affect its linearity. Further, the coefficient of inverse swaps was determined, which is an important indicator for assessing the risks and stability of the margin trading protocol. The process of position liquidation, which is an important component of the margin trading protocol, was considered separately, and finally the choice of the maximum allowable leverage was substantiated.

The practical significance of the results is to ensure the efficient and stable functioning of the margin trading protocol. The choice of the optimal maximum leverage is an important aspect for ensuring security and avoiding risks for market participants.

BLOCKCHAIN, FINANCIAL PROTOCOLS, CONSTANT SUM PROTOCOL, LIQUIDATION CONDITION, MAXIMUM ALLOWABLE LEVERAGE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CSM — Constant Sum Market

DeFi — Decentralized Finance

AMM — Автоматизовані маркет-мейкери

DEX — децентрализована біржа

LP — пул-ліквідності

BF — borrowing fee(комісія за користування кредитом)

BAR — Borrow annual rate(річна ставка за кредитом) P2P — peer-to-peer

P2C — peer-to-contract

ВСТУП

Актуальність дослідження. У 21 столітті набула популярності нова сфера фінансів та цифрових коштів – *блокчейн*. Технологія блокчейн використовується для створення незмінного або невизначеного реєстру для відстеження замовлень, платежів та інших транзакцій, з вбудованими механізмами для запобігання несанкціонованому введенню транзакцій і для забезпечення узгодженості в загальному представленні транзакцій. Технологія блокчейн існувала і раніше, але з появою криптовалюти увага до неї сильно збільшилася.

Чому саме блокчейн став популярним?

1) Немає єдиної бази зберігання даних. Усі записи зберігаються у кожного учасника системи.

2) Будь-який учасник може відстежити всі транзакції, що проходили в системі.

3) Транзакції відбуваються швидко та з мінімальними комісіями.

4) Всі дані зберігаються в зашифрованому вигляді. Користувач може відстежити всі транзакції, але не може ідентифікувати одержувача або відправника інформації, якщо він не знає номера гаманця.

Протягом багатьох років основою ринку були централізовані біржі, які мали швидкі розрахунки, великий обсяг торгів і постійне зростання ліквідності. Згодом з'явились ще й децентралізовані біржі, побудовані у вигляді протоколів, які не потребують довіри. На відміну від централізованих бірж, що покладаються на книгу ордерів, децентралізовані біржі покладаються на автоматизованих маркет-мейкерів або смарт-контракти, які створюють пули ліквідності токенів і встановлюють ціни відповідно до математичних формул. Одним з яких є Constant Sum.

Метою дослідження є вибір та обгрунтування параметрів(наприклад, максимально допустимого плеча) для безпечного

функціонування протоколу на базі моделі Constant Sum та формулювання умови ліквідації маржинальної позиції. Для досягнення мети необхідно розв'язати **задачу дослідження**, а саме описати даний метод і його застосування до вибору параметрів Constant Sum, аналізуючи різні зв'язки між параметрами протоколу та ризиками. Такий вибір параметрів має забезпечити стабільну роботу протоколу і знизить ризики до деякого заданого рівня, а також допомогти в розробці нових методів оцінювання та удосконаленні існуючих.

Для розв'язання задачі необхідно вирішити такі завдання:

1) Дослідження літератури щодо різних моделей функціонування децентралізованих фінансових протоколів.

2) Аналіз моделі Constant Sum.

3) Формулювання тверджень щодо властивостей цієї моделі та доведення цих тверджень.

4) Використання отриманих результатів для визначення параметрів функціонування цієї моделі та умови ліквідації.

5) На базі отриманих результатів, обчислення можливих чисельних значень для допустимого плеча.

Об'єктом дослідження є процес функціонування протоколу децентралізованих фінансів, що базується на моделі Constant Sum.

Предметом дослідження є вибір та обґрунтування максимально допустимого кредитного плеча та інших параметрів для моделі Constant Sum.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: теорії ймовірностей, математична статистика.

Наукова новизна отриманих результатів полягає в тому, що вперше запропоновано математичне обгрунтування методу вибору максимального допустимого кредитного плеча та умови ліквідації для вказаної моделі.

Практичне значення результатів полягає в тому, що вибір максимального допустимого кредитного плеча є важливим аспектом для забезпечення безпеки та уникнення ризиків для учасників ринку, це

значно зменшує ризики недооцінки операції та використання неоптимальних стратегій маркет-мейкінгу.

1 ОСНОВНІ ТЕОРЕТИЧНІ ПОНЯТТЯ БЛОКЧЕЙНУ

У цьому розділі буде представлено принципи роботи блокчейну та деяких протоколів, які адаптують базові принципи блокчейну до конкретних галузей або додатків.

Опишемо загальні поняття та ідеї роботи DEX, DeFi, Smart-contract, Chainlink, dApp, протоколів AAve, Compound, Uniswap та AMM.

1.1 Опис технології блокчейн

Концепція блокчейну бере свій початок у 1991 році, коли Скотт Сторнетта та Стюарт Хабер представили ідею криптографічно безпечного ланцюжка. Після двох десятиліть використання технологія набула популярності та широкого застосування. У 2008 році Сатоші Накамото надав технології встановлену модель і запланованe застосування. Перший блокчейн та криптовалюта були офіційно запущені у 2009 році, розпочавши шлях впливу блокчейну на всю технологічну сферу.

Означення 1.1. *Блокчейн* – база даних, яка містить записи про всі транзакції учасників системи. Ця база не має єдиного центру і керуючих органів. Замість таблиць, ця технологія групує дані у блоки; при заповненні інформацією блока, блок прив'язується до попередніх, створюючи певний ланцюг.

Блокчейном керують люди, які їм користуються. Оскільки всі учасники блокчейн-мереж рівноправні, транзації відбуваються безпоседерньо між ними. Кожен користувач має можливість відстежувати всі транзації, які відбулися, а блокчейн, у свою чергу, зберігає всю історію, без можливості змін та редагування. Також слід зазначити, що блокчейн децентралізований, тому актуально ввести означення смарт-контракту.

Означення 1.2. *Смарт-контракт* – це запрограмований цифровий контракт із заздалегідь прописаними умовами. Він дозволяє учасникам транзакцій безпечно обмінюватись грошима, акціями та іншими активами напряму, без участі посередників.

Цю концепцію було введено в блокчейн із введенням Ethereum. Основною задачею смарт-контракту є повна автоматизація договірних відносин між учасниками певної транзації. Якщо ж умови домовленостей не виконуються, то розумний контракт накладає певні штрафи або ж автоматично закриває учасникам доступ до активів. Смарт-контракти мають широкий акпект використання в різних сферах, проте розглядаючи саме блокчейн, смарт-контракт використовується всюди, від продажу токенів до управління децентралізованими організаціями, зберігаясь в блокчейні як і будь-яка інша криптовалютна транзакція. Неабияким недоліком смарт-контрактів є їх обмеженість. Вони можуть виконувати операції та обробки даних лише в межах блокчейну. Якщо смарт-контракт призначений для виконання угод за межами блокчейна, тоді на допомогу приходить оракул [8].

Означення 1.3. *Оракул* – це алгоритм, який запитує, перевіряє й автентифікує всі свідчення зовнішніх джерел, а потім відправляє їх у смарт-контракт.

Блокчейн-оракули допомагають інтегрувати блокчейн-технології в повсякденне життя і наблизити їхнє масове прийняття, скажімо такий собі посередник між блокчейном та реальністю. Кожен вид оракула класифікується за принципом роботи, джерелам одержуваних даних та ін. Програмний оракул бере інформацію з онлайн-джерела та передає її у блокчейн. Апаратний зчитує дані з фізичних ресурсів. Централізований контролюється одним лицем та є єдиним постачальником інформації для смарт-контракту. Децентралізований оракул об'єднує безліч оракулів.

Для останнього було розроблено Chainlink.

Означення 1.4. *Chainlink* – ринок оракулів, децентралізованих

постачальників даних, які передають дані та іншу інформацію в блокчейн.

Chainlink працює над отриманням доступу до різних вхідних даних, що розширює можливості застосування смарт-контрактів за межі блокчейна.

Рисунок 1.1 – Підключення оракулів до смарт-контрактів

Як децентралізована мережа, Chainlink складається із взаємопов'язаних комп'ютерів (також званих вузлами), які використовують оракул для збору даних із різних джерел [10].

Коли смарт-контракт на блокчейні відправляє запит на інформацію, створюється смарт-контракт SLA, який стає угодою про рівень обслуговування. SLA створює ще три свої субконтракти:

1) Reputation Contract перевіряє достовірність та справжність вузла, що надає дані.

2) Order-Matching Contract доставляє запит інформації вузлам та вибирає вузли, які будуть виконувати завдання.

3) Aggregation Contract перевіряє і погоджує всю отриману інформацію на предмет точності.

1.2 Поняття фінансових протоколів

Для того, щоб ще більше наблизитись до розкриття теми даної роботи, потрібно чітко розуміти поняття фінансових протоколів блокчейну, насамперед, що таке DeFi.

Означення 1.5. *DeFi (Decentralized Finance)* – фінансові послуги, що функціонують на протоколах першого рівня, таких як Ethereum, і пропонують користувачам доступ до відкритої та ефективної фінансової системи.

Основна мета полягає в тому, щоб послабити довіру до наявних інститутів і створити децентралізовані та більш інклюзивні версії фінансового забезпечення в мережах без обмежень. За допомогою смарт-контрактів платформи DeFi виключають участь посередників, що вкрай важливо для користувачів, яким недоступні банківські сервіси в рамках нинішніх систем. Йдеться про відмову від єдиних центрів управління та посередників на користь розподілу обов'язків серед учасників ринку. Наприклад, замість банків у DeFi кредити видають користувачі, які хочуть заробляти на своїх грошах. Так, зокрема, працює Compound. На ринку DeFi ціннник формують самі учасники ринку, які змушені слідувати за попитом [3].

Платформи DeFi охоплюють усе: від децентралізованих бірж (DEX, таких як Uniswap) до синтетичних активів, пулів ліквідності, страхових продуктів, платежів, протоколів запозичення/кредитування (наприклад, Compound), стейблкоїнів та багато чого іншого. Ці платформи функціонують аналогічно наявним фінансовим послугам, але здебільшого замінюють наявні інститути (наприклад, біржі) серією смарт-контрактів, що працюють на мережах.

Протокол Uniswap використовує автоматизованих маркет-мейкерів (AMM), які, по суті, є роботами, що котирують ціни між двома торговими активами. На перший погляд ця концепція може здатися складною, але

на практиці вона досить проста.

DEX, подібні до Uniswap (з AMM), просто замінюють книгу ордерів біржі смарт-контрактом, який котирує ціни між усіма учасниками пулу ліквідності для різних активів.

Безпосередньою проблемою, що виникає на багатьох платформах DeFi (наприклад, DEX), є ліквідність. Протоколи DeFi усвідомлювали, що фінансові інструменти і торгівля стануть першою великою технологічною приманкою криптовалютного ринку, але забезпечення ліквідності залишається складним завданням.

З розвитком децентралізованих програм DeFi, стрімко набули популярності децентралізовані біржі (DEX) із протоколами автоматизованого маркет-мейкера (AMM).

Означення 1.6. *Децентралізована біржа(DEX)* – це біржа, яка працює на основі розподіленого реєстру, не зберігає кошти та персональні дані користувачів на своїх серверах, а виступає лише як платформа для узгодження заявок на купівлю або продаж активів користувачів.

Торгівля на таких платформах відбувається безпосередньо між учасниками (peer-to-peer) без будь-яких фінансових посередників.

DEX використовують смарт-контракти для визначення цін на криптовалюту за допомогою алгоритмів.

DEX пропонують практично безмежний вибір токенів, від добре відомих до дивних і абсолютно випадкових. Це тому що будь-хто може випустити токен на основі Ethereum і створити для нього пул ліквідності. Розробка DEX здійснюється з акцентом на інновації та розвиток. Через це вони здебільшого мають відкритий код, тож кожен може адаптувати код для створення нових конкуруючих проектів. Зараз нові проекти створюються на базі існуючої біржі (наприклад, Uniswap). Завдяки цьому нові проекти створюються на базі вже існуючих бірж (наприклад, за допомогою Uniswap).

Саме тому DEX-біржі більш безпечні, адже немає єдиної бази даних, в якій зберігаються всі дані, і кожен користувач самостійно керує своїми

ключами. Біржа не зберігатиме їх на біржі з будь-якою метою.

У світі існує багато різних типів DEX, але одним із найпопулярніших є Automated Market Maker (AMM) DEX, як Uniswap. Під час розробки децентралізованої біржі криптовалют можна використовувати автоматизованих маркет-мейкерів або смарт-контракти, які створюють пули ліквідності для криптовалют і встановлюють ціни відповідно до розрахованих математичних формул [4].

Означення 1.7. *Автоматизовані маркет-мейкери (AMM)* – це протоколи, які забезпечують ліквідність на певних ринках за допомогою автоматичної алгоритмічної торгівлі.

Наприклад, у контексті децентралізованих торгових систем криптовалют автоматизовані маркетмейкери — це смарт-контракти. Щоб створити такі пули ліквідності, вони створюють так звані пули ліквідності токенів, які автоматично торгуються за допомогою алгоритму, а не за допомогою книги ордерів [9].

Означення 1.8. *Маркет-мейкинг* – процес забезпечення ліквідності фондового ринку шляхом одночасного встановлення цін як для купівлі, так і для продажу, а організації, які надають цю послугу, називаються *маркет-мейкерами.*

Роль маркет-мейкера полягає в тому, щоб зробити фінансові ринки більш ефективними і знизити волатильність цін на активи, забезпечуючи постійну ліквідність для активів.

Розумний контракт автоматично надсилає токени в пул ліквідності, а потім обмінює їх на аналогічні токени з пари. У випадку, коли користувач вирішив торгувати на децентралізованій біржі, яку реалізує AMM, щоб заробляти на ній гроші, обмінний курс між токенами розраховується автоматично за математичною формулою, яка була використана у вигляді однієї або двох простих формул. Наприклад, формула, яку використовує AMM Uniswap:

$$x * y = k,$$

де x і y –кількість кожного токена в пулі, а k – зумовлена константа, що зберігає те саме значення. Це просто в реалізації і дозволяє ефективно агрегувати ліквідність, але й означає, що значна частина активів, що зберігаються в пулі, ніколи не буде задіяна.

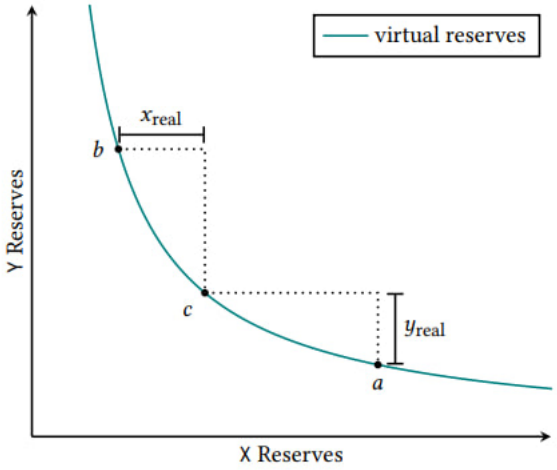

Рисунок 1.2 – Постійний пул з віртуальними резервами

Зокрема, позиція повинна мати достатню кількість активу , щоб покрити рух ціни до її верхньої межі. Аналогічно, позиція повинна мати достатню кількість активу Y, щоб покрити рух ціни до його нижньої межі. На рисунку 1.2 зображено цю залежність для позицій та поточної ціни. Коли ціна виходить з діапазону позиції, ліквідність позиції більше не є активною і більше не приносить комісійних. У цей момент її ліквідність повністю складається з одного активу, тому що резерви іншого активу повинні бути повністю виперпані. Якщо ціна коли-небудь повертається в діапазон, то ліквідність знову стає активною [6].

Незважаючи на те, що AMM підвищує ліквідність токенів, більшість AMM вкрай неефективні з погляду капіталу: більша частина коштів, які перебувають у них на поточний момент, не використовується. Це пов'язано з особливостями моделі, про яку йшла мова вище. Іншими словами: чим

більше ліквідності в пулі, тим більші ордери система може підтримувати в більшому ціновому діапазоні.

Означення 1.9. *Пул-ліквідності(LP)* – сукупність криптовалютних токенів, заблокованих у смарт-контракті.

Пули ліквідності є невід'ємною частиною AMM та децентралізованої торгівлі в цілому. Для участі на цьому ринку, користувач має додати вартість двох токенів у пул, щоб створити ринок. А як винагороду, за надання власних коштів, постачальник ліквідності отримує комісії від угод, які відбуваються в пулі, пропорційно його часті в загальному обсязі ліквідності.

На пули ліквідності спираються багато децентралізованих бірж, таких як Uniswap. І оскільки постачальником ліквідності може стати хто завгодно, AMM зробили ринок доступнішим. Зацікавленість дана концепція набула завдяки популіризації Uniswap. Після чого пули ліквідності почали використовуватись і на інших популярних біржах – SushiSwap, Curve і Balancer. в пулях на цих платформах знаходяться токени ERC-20.

Окрім отримання комісії за протоколи, токени управління являються ще одним джерелом прибутку для постачальників ліквідності, так як вони надають певні права під час змін у протоколах або права на частину прибутку протоколу.

Коли користувач укладає угоду з AMM, у нього немає контрагента в традиційному сенсі цього слова. Замість цього він здійснюєте операцію проти ліквідності в пулі ліквідності. Для здійснення покупки покупцеві не потрібна наявність продавця, необхідна лише достатня ліквідність у пулі. Трейдери можуть входити і виходити з позицій у парах токенів, які можуть бути вкрай неліквідними на біржах з OrderBook. Біржу з ордербуком можна вважати одноранговою біржею, де покупці і продавці пов'язані ордербуком, угоди відбуваються безпосередньо між гаманцями користувачів.

Незважаючи на вагомі переваги, AMM часто характеризуються

високим ковзанням і втратою від дивергенції, двома неявними економічними ризиками, що накладаються на кошти користувачів біржі та LP відповідно. Крім того, DEX на основі AMM пов'язаний із безліччю проблем безпеки та конфіденційності. Тому останні роки з'являються нові протоколи, які намагаються удосконалювати ринок блокчейну та вводити новітні іноваціх в цю сферу. Протоколи AMM складаються практично з однакового набору механізмів, які дозволяють реалізовувати численні функціональні задачі бірж; відмінності переважно полягають у виборі параметрів та адаптації механізму.

1.3 Фінансові протоколи та платформи блокчейна

В попередніх підрозділах вже зачіпали теми Uniswap, Маркет-мейкерів, Compound та Aave. Тому далі буде більш детально розібрано з їх принципами роботи.

Означення 1.10. *Uniswap* – автоматизований протокол ліквідності, в якому для виконання угод не потрібні книги ордерів або інша централізована сторона.

Uniswap дозволяє торгувати без посередників, зберігаючи при цьому високий ступінь децентралізації. Тут немає книги ордерів, тут використовується модель Constant Product Market Maker (маркет-мейкер з постійним продуктом), який є одним з маркет-мейкерів AMM, але про нього поговоримо згодом.

Uniswap v3 – це одна з технологій, що лежить в основі Uniswap. Команда Uniswap задумалась над тим, щоб створити технологію за допомогою якої можна буде зменшити кількість неактивної ліквідності, тому і був створений Uniswap v3 [2].

Однією з пріоритетних особливостей між іншими технологіями є ефективність використання капітала. В якійсь мірі, Uniswap v3 – це спосіб створення ончейн-книги ордерів на Ethereum, де маркет-мейкери можуть

ухвалювати рішення про надання ліквідності у встановлюваних ними цінових діапазонах. Ключова перевага AMM у тому, що кожен може забезпечити ліквідність і змусити свої кошти працювати.

Оскільки кожен може встановлючати собі цінові діапазони, тому пул-ліквідність в Uniswap можна вважати не взаємозамінною. Однією з переваг подання LP-позиції в Uniswap як взаємозамінного токена була б можливість її використання в інших частинах DeFi. LP-токени в Uniswap v2 можна вносити в Aave або MakerDAO як забезпечення. В Uniswap v3 так уже зробити не можна, оскільки кожна позиція унікальна.

Uniswap став одним із найбільш широко використовуваних і популярних DEX в екосистемі DeFi, а також став широко використовуваним інструментом для створення нових активів, нових пулів і для торгівлі активами для різних цілей. Деякі інші проекти також були створені з використанням кодової бази Uniswap, але добавши більш прибавливі умови для користувачів.

Означення 1.11. *Aave* – це лендинговий DeFi-протокол, що дає змогу позичати і займати криптоактиви з використанням змінних і стабільних процентних ставок.

1 травня 2017 року Кулечов заснував компанію ETHLend. У листопаді 2017 року ETHLend запустила лендингову P2P-платформу ETHLend.io і провела ICO на $16,2 млн. Проєкт продав 1 млрд нативних токенів LEND. 300 млн монет (23%) отримали засновник і команда [5].

У перекладі з фінської Aave означає "привид". Як пояснюють засновники протоколу "бренд продовжує інтригувати користувачів інноваційними технологіями і націлений на створення прозорої та відкритої інфраструктури для децентралізованих фінансів". ETHLend стала дочірньою компанією Aave.

Спочатку платформа працювала за принципом однорангової моделі (P2P), де користувачі взаємодіяли зі смарт-контрактами. Проте, не завжди знаходяться контрагенти і ліквідність для ефективного здійснення операцій. Застовників таке не влаштовувало, тому вони

вирішили перейти до моделі peer-to-contract (P2C), яку використовує більшість протоколів DeFi.

На P2C-платформі кошти депонуються за допомогою спеціального контракту, який дає змогу моментально позичити криптоактиви зі сплатою відсотків за користування кредитними коштами.

На платформі взаємодіють учасники двох категорій: позичальники і кредитори.

Запозичення. Користувачі депонують в Aave активи, що використовуються як заставне забезпечення. В обмін на це вони можуть взяти в борг меншу суму активу, що визначається коефіцієнтом "кредит/вартість застави"(Loan to Value, LTV).

Коефіцієнт "кредит/вартість застави"розраховується для кожної застави індивідуально і виражається у відсотках. Як забезпечення користувачі можуть надавати будь-який з доступних на платформі токенів.(див. рисунок 1.3)

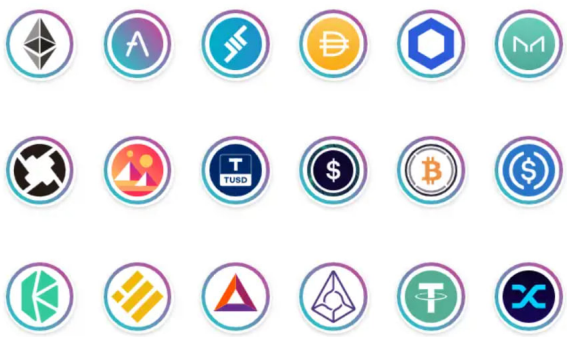

Рисунок 1.3

Aave стала першою лендинговою платформою, яка дала користувачам можливість позичати і позичати USDT. AMM пул ліквідності (AMM Liquidity Pool) дає змогу постачальникам ліквідності Uniswap і Balancer використовувати їхні LP-токени як заставне забезпечення в Aave Protocol.

Кредитування. Кредитори вносять свої кошти в "пул з якого користувачі можуть потім брати позики. Кожен пул відкладає невеликий

відсоток активу в якості резерву, щоб допомогти застрахуватися від будь-якої волатильності в рамках протоколу. Це також зручно дозволяє кредиторам вилучати свої кошти в будь-який час.

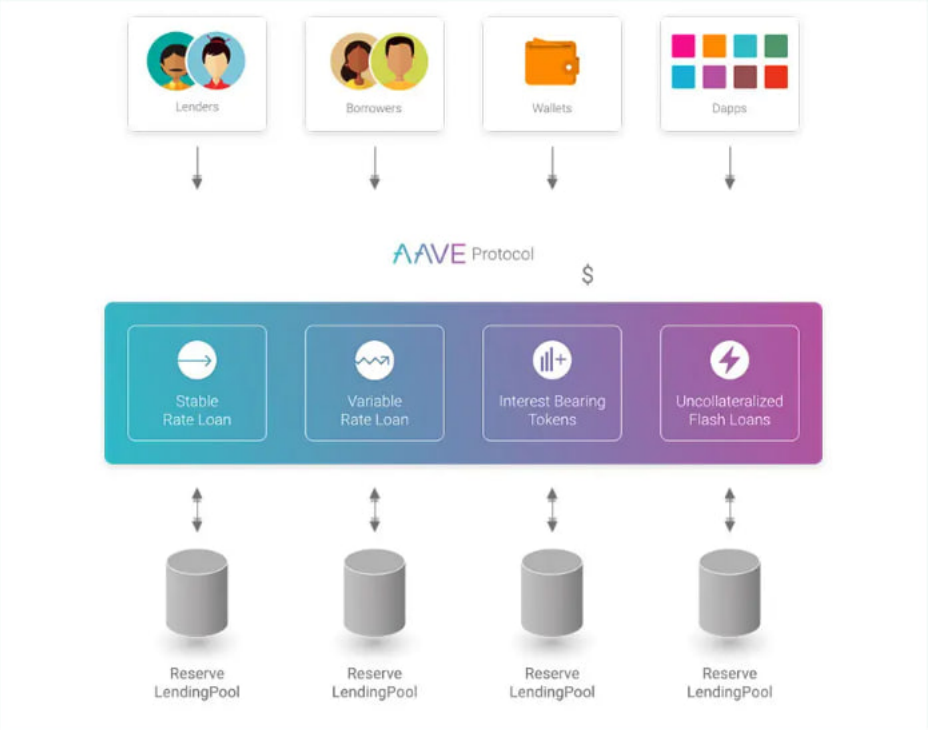

Рисунок 1.4 – Як працює протокол Aave

Aave пропонує дві процентні ставки: стабільну та змінну. Змінна процентна ставка визначається алгоритмічно на основі коефіцієнта використання пулу активів (іншими словами, попиту), де збільшення коефіцієнта використання даного пулу призводить до збільшення процентних ставок як для кредиторів, так і для позичальників (і навпаки).

Стабільна процентна ставка – це середнє за останні 30 днів значення процентних ставок за активом. Цю історію процентних ставок можна побачити при кредитуванні або позичанні активу на платформі. Перемикатися між стабільною і змінною ставкою можна в будь-який момент (для цього потрібно лише сплатити невелику комісію за газ ETH).

Найвідоміший внесок Aave в DeFi є створення флеш-позики(*Flash loans*). Це такий собі швидкий та небезпечний кредит, який можна

отримати, щоправда, дуже ненадовго. Він видається практично миттєво, однак і повернути його треба дуже швидко. Кошти треба повернути до моменту видобутку наступного блоку Ethereum – це 13 секунд. Таким чином, флеш-кредит Aave "живе"в рамках 13-секундного періоду: якщо позичальник не встиг повернути кошти, то транзакція анулюється. Це зручно, тому що в результаті не ризикує жодна зі сторін – ні сама платформа, ні позичальник [12].

Флеш-кредити дозволили криптовалютним трейдерам зробити цілу купу дивацтв, в першу чергу, фермерство дохідності. Вони є ключем до знаменитої техніки Compound yield farming в рамках InstaDapp, агрегатора протоколів DeFi.

Aave – це надзвичайно перспективний проект, який, схоже, залишився дещо поза увагою. У порівнянні з іншими протоколами DeFi-кредитування, він пропонує арсенал функцій, активів та інструментів розробки, які дозволяють іншим впроваджувати ці ж функції у власні DeFi-проекти.

Означення 1.12. *Compound* – це протокол децентралізованих фінансів (DeFi) на блокчейні, у стінах якого користувачі можуть позичати і займати цифрові активи без посередників. На платформі можна працювати анонімно.

Усю криптовалюту Compound Finance зберігає в смарт-контрактах, з якими користувачі можуть взаємодіяти безпосередньо. За блокування цифрових активів під потреби Compound Finance система платить користувачам відсотки. Роботу в такому форматі називають DeFi-стейкінгом. Інструменти Compound Finance інтегровані в багато популярних на ринку цифрових активів платформ. Наприклад, заробляти на блокуванні активів у децентралізованому протоколі можна через криптобіржу Binance.

Aave і Compound є протоколами криптовалютного кредитування з надлишковим забезпеченням і працюють фактично однаково. Обидва об'єднують активи кредиторів у кредитні пули, з яких позичальники

DEFI PULSE	Name	Chain	Category	Locked (USD) ▼	1 Day %
1.	Compound	Ethereum	Lending	$629.4M	1.12%
2.	Maker	Ethereum	Lending	$539.0M	1.96%
3.	Aave	Ethereum	Lending	$125.3M	2.61%
4.	InstaDApp	Ethereum	Lending	$85.2M	1.19%
5.	dYdX	Ethereum	Lending	$33.9M	1.24%

Рисунок 1.5 – Топ-5 протоколів кредитування в DeFi

можуть брати кредити, обидва мають власний токен управління і разом з MakerDAO є найбільшими протоколами в DeFi за обсягом "активів під управлінням"(AUM). При цьому Compound набагато менш складний і, відповідно, не пропонує стільки можливостей, як Aave.

Aave пропонує стабільні відсоткові ставки, Compound – ні. Aave дозволяє перемикатися між стабільною та змінною процентною ставкою, а Compound – ні. Aave пропонує кредити на першу вимогу, а Compound ні. Aave має 17 активів для кредитування та запозичення, а Compound - 9. Найкраще те, що Aave дозволяє користувачам позичати більший відсоток від базової застави (75% проти 66,6% у Compound).

На папері здається, що Aave об'єктивно кращий за Compound як протокол криптовалютного кредитування. Однак є дві основні переваги Compound перед Aave. Перша полягає в тому, що він набагато зручніший у використанні.

Той факт, що він не пропонує так багато функцій, принципово полегшує його розуміння і навігацію для нових користувачів. По-друге, Compound дає користувачам набагато більше стимулів для участі в протоколі, надаючи як кредиторам, так і позичальникам невелику частину токенів COMP кожні кілька секунд.

І нарешті, обґрунтувавши усі базові поняття про блокейн, перейдемо до теми *Constant Sum*.

Автоматизовані маркет-мейкери (AMMs) – це тип децентралізованих бірж (DEX), які використовують алгоритмічні

"грошові роботи щоб полегшити індивідуальним трейдерам купівлю та продаж криптоактивів. Замість того, щоб торгувати безпосередньо з іншими людьми, вони працюють на основі смарт-контрактів і,таким чином, дозволяють здійснювати швидкі та безпечні обміни без спеціальних книг замовлень. Під час купівлі монети трейдера вносяться до пулу ліквідності й обмінюються на інший токен пари.

AMM набули ще більшої популярності після створення нової моделі Constant Function Market Maker (CFMM), що дозволила подальше застосування до цифрових активів [11].

Різновиди маркет-мейкерів:

1) Constant Function (CFMM) – популярний, функціонує постійно.

2) Constant Product (CPMM) – може регулювати діапазони цін.

3) Constant Mean (CMMM) – може обробляти більше 2-х пар криптовалют одночасно.

4) Constant Sum (CSMM) – рідко використовується, єдиним незмінним значенням залишається сума активів.

Маркет-мейкери з постійною функцією (CFMM), такі як Constant roduct market makers, Constant sum market makers, and Constant mean market makers, є класом AMM першого покоління, які стали популярними завдяки таким протоколам, як Bancor, Curve та Uniswap. Ці AMM-обміни базуються на постійній функції, де сукупні резерви активів торгових пар повинні залишатися незмінними. У некастодіальних AMM депозити користувачів по торговим парам об'єднуються в рамках смарт-контракту, який будь-який трейдер може використовувати для забезпечення ліквідності токен-свопів. Користувачі торгують проти смарт-контракту (об'єднаних активів), а не безпосередньо з контрагентом, як на біржах з книгою заявок.

CPMM

Першим типом CFMM, що з'явився, був постійний маркет-мейкер продукту (CPMM), який був популяризований першим DEX на основі AMM, Bancor. В основі CPMM лежить функція $x * y = k$, яка

встановлює діапазон цін на два токени відповідно до наявних кількостей (ліквідності) кожного токена. Коли пропозиція токенів X збільшується, пропозиція токенів Y повинна зменшуватися, і навпаки, щоб підтримувати постійний добуток K .Якщо побудувати графік, то вийде гіпербола, де ліквідність завжди доступна, але за дедалі вищими цінами, які з обох кінців наближаються до нескінченності.

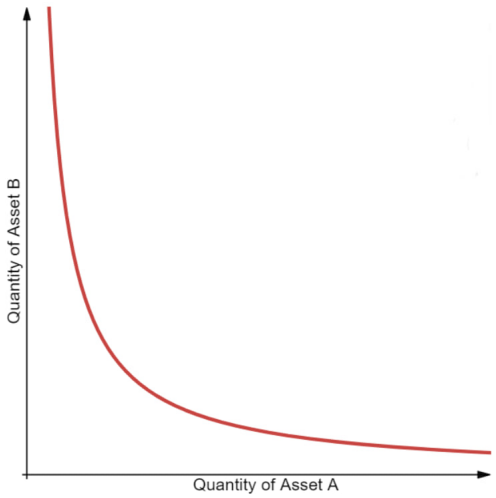

Рисунок 1.6 – Візуалізація CPMM

CSMM

Другий тип – маркет-мейкер з постійною сумою (CSMM), який ідеально підходить для угод з нульовим впливом на ціну, але не забезпечує нескінченну ліквідність. CSMM працюють за формулою $x + y = k$, яка створює пряму лінію на графіку. Така конструкція, на жаль, дозволяє арбітражникам злити один з резервів, якщо позамережева довідкова ціна між токенами не становить 1:1. Така ситуація руйнує одну сторону пулу ліквідності, залишаючи всю ліквідність лише в одному з активів і, таким чином, не залишаючи більше ліквідності для трейдерів. Через це CSMM є моделлю, яка рідко використовується AMM.

CMMM

Третій тип – маркет-мейкер з постійним середнім значенням (CMMM), що дозволяє створювати AMM, які можуть мати більше двох

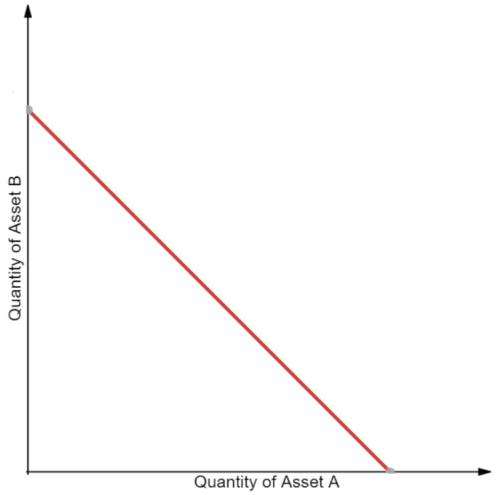

Рисунок 1.7 – Візуалізація CSMM

токенів і зважуватися поза стандартним розподілом 50/50. У цій моделі середньозважена геометрична величина кожного резерву залишається постійною. Для пулу ліквідності з трьома активами рівняння буде наступним: $(x * y * z)^{\frac{1}{3}} = k$.

Це дозволяє варіювати ризики за різними активами пулу та уможливлює свопи між будь-якими активами пулу.

Багато моделей управління активами першого покоління обмежені непостійними збитками та низькою ефективністю використання капіталу, що впливає як на постачальників ліквідності, так і на трейдерів.

Традиційні моделі управління активами та пасивами вимагають великих обсягів ліквідності для досягнення такого ж рівня впливу на ціну, як і біржа, що базується на книзі заявок. Це пов'язано з тим, що значна частина ліквідності AMM стає доступною лише тоді, коли цінова крива починає набувати експоненціального характеру. Через надзвичайний вплив ціни більша частина ліквідності ніколи не буде використана раціональними трейдерами.

Причина цього полягає в тому, що постачальники ліквідності AMM не контролюють, які ціни пропонують на ринку деякі люди, що змушує їх часто називати це «лінивою ліквідністю, яка недостатньо використовується та погано забезпечена». Маркет-мейкери на біржі ордерів можуть точно

контролювати ціни, за якими купувати та продавати токени. Це призводить до дуже високого рівня використання капіталу, але з компромісом у формі активної участі та контролю за забезпеченням ліквідністю.

Висновки до розділу 1

В цьому розділі було розглянуто всі базові поняття блокчейну, а також різних DeFi протоколів, бірж, платформ та моделей. Було проаналізовано наступні децентралізовані обміни та DeFi протоколи: Aave, Compound, Uniswap, AMM; а також різні типи смарт-контрактів DEX та DeFi протоколів. Досліджено переваги та недоліки кожного протоколу та моделі зазначених вище та проведено порівняльну характеристику деяких протоколів. Розглянуто основні поняття AMM та їх різновидів, після чого увагу було зосереджено на Constant Sum, який є центральною точкою цієї роботи. У наступному розділі цей протокол будете проаналізовано більш детально з математичної точки зору.

2 ПРОТОКОЛ CONSTANT SUM

В цьому розділі проведено аналіз існуючих протоколів децентралізованої маржинальної торгівлі; наведено опис моделі Constant Sum та обгрунтування вибору даної моделі для цього дослідження та основні позначень та взаємозв'язків, які використовуються для дослідження даної теми.

2.1 Аналіз існуючих протоколів децентралізованої маржинальної торгівлі

DeFi змінює гру в галузі фінансів, дозволяючи користувачам здійснювати фінансові операції без посередництва традиційних фінансових установ. Різні типи DeFi надають користувачам більше можливостей для керування своїми фінансами та забезпечення їх безпеки.

DeFi дозволяє користувачам здійснювати фінансові операції в безпечному та автономному середовищі, використовуючи технологію блокчейн. Це дає користувачам більше контролю над їхніми фінансами та дозволяє їм уникнути недоліків традиційних фінансових установ, таких як високі комісії та обмеження доступу до фінансових послуг. Більше того, DeFi може допомогти зменшити глобальну нерівність у доступі до фінансових послуг, забезпечуючи фінансову включеність для всіх користувачів, незалежно від їхнього місцезнаходження чи соціального статусу.

Протоколи DeFi мають багато спільних рис, але також мають свої відмінності. Однією з найбільш очевидних спільних ознак є те, що ніхто не контролює протокол, і він працює на основі коду, який доступний для перевірки та опублікування. Також вони дозволяють користувачам безпосередньо взаємодіяти між собою, минувши посередників, які

зазвичай здійснюють контроль над фінансовими операціями. Це дає користувачам більшу свободу та безпеку виконання операцій.

Ще одною спільною ознакою протоколів DeFi є використання криптовалют. Це дозволяє забезпечити високу швидкість операцій та знизити витрати на транзакції. Крім того, використання криптовалют забезпечує анонімність та конфіденційність операцій, що є важливим для багатьох користувачів.

Однак, протоколи DeFi також мають свої відмінності. Умовно всі протоколи DeFi можна розділити на 5 типів, кожен з яких має свої особливості та переваги.

1. **Протоколи обміну**. Це найбільш відомий та використовуваний тип протоколів DeFi. Вони дозволяють користувачам обмінювати одну криптовалюту на іншу без посередників. Протоколи обміну, такі як Uniswap та Sushiswap, базуються на концепції автоматичного ринку та використовують ліквідність для здійснення операцій.

2. **Протоколи ставок**. Вони дозволяють користувачам заробляти проценти на своїх криптовалютних активах. Вони використовуються в основному для зберігання та збільшення капіталу. Протоколи ставок, такі як Aave та Compound, використовують механізм позик та вкладень для забезпечення прибутків для користувачів.

3. **Протоколи страхування**. Дозволяють забезпечити захист від можливих ризиків, пов'язаних з криптовалютними інвестиціями. Вони забезпечують фінансовий захист та надійність криптовалютних інвестицій. Протоколи страхування, такі як Nexus Mutual та Opyn, дозволяють користувачам захищати свої активи від можливих ризиків.

4. **Протоколи синтетичних активів**. Дозволяють користувачам створювати та торгувати інструментами, які пов'язані з реальними активами. Такі протоколи, як Synthetix, дозволяють створювати синтетичні версії реальних активів, таких як акції та золото, і торгувати ними на блокчейні.

5. **Протоколи управління активами**. Дозволяють користувачам

ділитися своїми криптовалютними активами з іншими користувачами, які бажають інвестувати в криптовалюти. Протоколи управління активами, такі як Yearn Finance та Balancer, дозволяють забезпечити автоматизований та оптимальний розподіл капіталу між різними криптовалютними проектами.

Кожен з цих типів протоколів DeFi дозволяє користувачам забезпечити свою фінансову свободу та незалежність, і використовується для різних цілей та завдань.

Однак ринок DeFi постійно змінюється, розширюється і з'являється велика кількість нових протоколів. А проблема в тому, що вибір параметрів протоколу, оцінка ризиків, взаємозв'язків та залежностей між ними представлені дуже стисло у всіх наукових і технічних публікаціях.

2.2 Обгрунтування вибору теми роботи

В даній роботі представлено метод вибору параметрів для протоколу маржинальної торгівлі Costant Sum, який може працювати з різними DEX і DeFi-платформами.

Власне протокол Constant Sum є одним з найбільш використовуваних методів оцінювання в анкетних опитуваннях, де респондентам пропонується розподілити задану суму між декількома альтернативами. Однак, не дивлячись на широке використання цього методу, його математичне обгрунтування є недостатньо дослідженим.

Дефіцит наукових публікацій на цю тему може призвести до некоректного застосування протоколу Constant Sum та, відповідно, до неточності результатів дослідження.

Тому основною метою моєї роботи є створення математичного методу, який дозволить обгрунтувати вибір параметрів для протоколу Constant Sum. У представленій роботі буде описано данний метод і його застосування до вибору параметрів Constant Sum, аналізуючи різні зв'язки між параметрами протоколу та ризиками. Такий вибір параметрів

має забезпечити стабільну роботу протоколу і знизить ризики до деякого заданого рівня, а також допомогти в розробці нових методів оцінювання та удосконаленні існуючих.

2.3 Опис протоколу Constant Sum

Constant Sum є протоколом, який дозволяє користувачам торгувати активами з використанням позикових коштів. Протокол базується на механізмі Constant Sum Market Maker (CSMM), який забезпечує ліквідність ринку та управління ризиками.

У Constant Sum обидві сторони вносять депозит в криптовалюті, який використовується для забезпечення відкритих позицій. Кожна сторона розміщує свою пропозицію про те, наскільки вартість активу зміниться за певний період часу.

У разі, якщо сторони домовляються про різні прогнози, то вони визначають ставки, які вони готові заплатити, якщо їхні прогнози виявляться невірними. Кожна сторона вносить до спільного кошторису суму, що дорівнює сумі депозитів обох сторін. Ця сума є гарантією, що у випадку порушення угоди з боку однієї зі сторін, інша сторона отримає компенсацію.

Коли період угоди закінчується, сторони порівнюють фактичну зміну вартості активу з їхніми прогнозами. Якщо прогноз однієї сторони виявляється точним, а іншої - ні, то сторона з точним прогнозом отримує зібрані в кошторисі кошти. Якщо обидві сторони помилилися, то кошти розподіляються між ними відповідно до внесених депозитів.

Протокол Constant Sum використовує механізм збалансованих позицій (balanced positions), що дозволяє управляти ризиками та забезпечувати ліквідність. Усі заявки на купівлю та продаж виконуються на ринковій ціні, яка змінюється в залежності від попиту та пропозиції.

2.4 Основні позначення та взаємозв'язки

Великі латинські літери – $(X, Y, Z, W \dots)$ використовуються для позначення типу активу. Відповідна величина активу, тобто кількість його одиниць, описується малими літерами $(x,y,z,w \dots)$.

Означення 2.1. Функцію

$$C_{X/Y}(t; x) \tag{2.1}$$

– яка в точці $(t; x)$ дорівнює кількості одиниць активу Y, які можна отримати в момент часу t, продавши x одиниць активу X. Така функція має назву *функція вартості активу.*

Ця функція, яка описується вартістю активу, може бути розрахована на основі середньої ринкової ціни і може залежати від інших параметрів, але поки що буде обмежена часом(в даній роботі, для поставленої задачі).

Розглянемо три активи X, Y та W. Активи X та Y завжди будуть різними. Актив W може бути рівним одну із активів X або Y, але не обов'язково. При відкритті торгової позиції з кредитним плечем трейдер використовує актив W (депозит), який у нього є в розмірі w_0 одиниць, позичає актив X в розмірі x одиниць, і обмінює їх (активи W і X) на y одиниць активу Y. Допустима кількість позиченого активу в одиницях визначається із співвідношення

$$x \leqslant l_{max} \cdot C_{W/X}(t_0,w_0), \tag{2.2}$$

де t_0 – час відкриття позиції, а l_{max} встановлюється заздалегідь.

Означення 2.2. Величина $L_{max} = l_{max}+1$ називається *максимально прийнятне кредитне плече.*

Надалі буде використовуватись позначення $w = C_{W/X}(t_0,w_0)$.

Означення 2.3. Відношеннння $L = \frac{w+x}{w}$ називається *максимально прийнятне кредитне плече.*

Зокрема, якщо актив депозиту W збігається з позиченим активом X, тоді $w = w_0$ та допустимий розмір визначається нерівністю $\frac{w+x}{w} = L \leqslant L_{max}$.

Означення 2.4. Значення w_0 називається *депозитом Трейдера.*

Взагалі кажучи, в залежності від різної торгівлі, після відкриття позиції депозит може бути заморожений і повернутий Трейдеру тільки після того, як він поверне одиницю позиченого активу X до пулу ліквідності, а також всі інші платежі за протоколом. Однак тут і далі ми припускаємо, що Трейдер використовує депозит разом з позиченим активом, а саме обмінює його на позицію по активу Y.

Депозит є своєрідною страховкою для Кредитора на випадок, якщо Трейдер недостатньо точно спрогнозує ринкові зміни і вартість активу Y впаде відносно вартості активу X або не зросте до очікуваного рівня. Депозит в такому випадку використовується для відшкодування Кредиторам вартості позиченого у них активу та плати за позику, передбаченої протоколом. При цьому сам протокол побудований таким чином, що при збільшенні ризиків позиція з кредитним плечем примусово закривається, гарантуючи повернення Кредиторам не тільки всіх позичених ними активів, але й плати за користування цими активами.

Після відкриття позиції актив X (разом з депозитом) обмінюється Трейдером на якийсь інший актив Y, який, як він сподівається, зросте в ціні по відношенню до актива X.

Можливі три випадки:

1) депозит знаходиться в активі X,

2) депозит знаходиться в активі Y,

3) депозит знаходиться в третьому активі W.

Згодом буде розглянуто випадок, коли актив депозита співпадає з активом Y.

Для кожного випадку кількість y активу Y, які отримуються після відкриття позиції, буде розраховуватися по-різному.

Нехай x_0 кількість одиниць активу X, яку Трейдер позичає під

депозит, та w_0 кількість одиниць активу W – їх депозит. Тоді, обмінявши позиченого активу та депозит (якщо $W \neq Y$) в актив Y, Трейдер отримує певну кількість y одиниць активу Y, що визначається за наступними формулами:

у випадку 1):

$$y = C_{X/Y}(0,x_0 + w_0), \tag{2.3}$$

у випадку 2):

$$y = C_{X/Y}(0,x_0) + w_0, \tag{2.4}$$

у випадку 3):

$$y = C_{X/Y}(0,x_0) + C_{X/Y}(0,w_0) \tag{2.5}$$

Як вже зазначалося, існує також потенційний випадок, коли актив знаходиться на депозиті W, такі, що $W \neq X$ і $W \neq Y$, «заморожується», і не переноситься до активу Y.

При цьому випадку 4):

$$y = C_{X/Y}(0,x_0) \tag{2.6}$$

але ми не будемо його тут розглядати.

Час, протягом якого позиція залишається відкритою, зазвичай вважається обмеженим (в цій роботі, припущено, що він обмежений 10 хвилинами).

2.5 Constant Sum Market

Почнемо з короткого пояснення маркет-мейкера з постійною сумою. Нехай цей маркет-мейкер складається з двох активів, X та Y, вартістю x та y одиниць, відповідно, де ціни цих двох активів, виражених в USDC або USDT, просто однакові. Грубо кажучи, ціна x одиниці активу X дорівнює y одиниць активу Y, або ціна однієї одиниці активу X складає $\frac{y}{x}$ одиниць активу Y, і навпаки.

Визначимо константу S як $S = x + y$.

Далі визначимо величину ρ, яка називається **комісією за транзакції**, що може бути виражена як у відсотках, так і у вигляді співвідношення, а також значення $\gamma = 1 - \rho$. Зауважимо, що значення ρ досить мале (Наприклад, для Compound $\rho = 0.003$), тому нерівність $\frac{1}{\gamma} = 1 + \frac{\rho}{1-\rho} > 1 + \rho$ можна переписати приблизно як $\frac{1}{\gamma} \approx 1 + \rho$.

Нехай деякий Трейдер хоче купити Δy одиниць активу Y. Тоді кількість Δx активу X, яку він повинен заплатити за нього, визначається з рівняння

$$(y - \Delta y) + (x + \gamma \Delta x) = S,$$

або $\Delta x = \frac{\Delta y}{\gamma}$, що при достатньо великому b і малому значенні Δy може бути апроксимовано рівністю

$$\Delta x \approx (1 + \rho) \cdot \Delta y, \tag{2.7}$$

використовуючи апроксимацію для $\frac{1}{\gamma}$ наведену вище. Співвідношення 2.7 пояснює, чому називається комісією за транзакції [7].

У теоремі 2.1 нижче буде доведено, що модель Constant Sum лінійна.

А отже, доцільно вважати, що дана модель підходить для криптовалют таких як стейблкоїни.

Означення 2.5. Стейблкоїни – це вид криптовалюти, ціна якої постійна, тобто вартість прив'язана до вартості "стабільного"резервного

актива, такого як, наприклад, USDC або USDT.

Розберемо це на прикладі.

Приклад 2.1. Кладемо в корзинку $S = 2\$ + 80UAH$ Хочемо обміняти 1\$ у гривні. Скільки гривень отримаємо?

Розв'язання $\Delta x = 1\$$

$\Delta y = \gamma \Delta a = \gamma \cdot 1$

Тобто отримаємо < 1 гривні.

Саме тому тут повинні бути стейблкоїни. Оскільки взявши для прикладу, шо у тут лежало

$S = 2USDT + 2USDC$

Тоді так, дійсно. Поклавши 1 USDT отримаємо майже 1 USDC, тобто майже однакову кількість з дуже крихітною комісією.

У теоремі 2.2 буде показано, що наступна оцінка справедлива для деяких $\mu \in (0,1)$:

$$C_{Y/X}(t; C_{X/Y}(t,x)) = \gamma^2 x, \tag{2.8}$$

де μ залежить від параметрів моделі Constant Sum Market . Зокрема, для моделі CSM $\mu = 0.994$.

2.6 Властивості функції вартості активів в Constant Sum

В цьому підрозділі буде сформульовано і доведено кілька нерівностей, які описують корисні властивості вартості активів за припущень CSMM.

Надалі будуть використовуватися всі позначення, наведені вище. Також визначено, що:

$\Delta_1 x$, $\Delta_2 x$ деякі суми активу X, і покладено $\Delta x = \Delta_1 x + \Delta_2 x$;

$\Delta_1 y$, $\Delta_2 y$ деякі суми активу Y, які отримують за торгівлю $\Delta_1 x$, $\Delta_2 x$, відповідно;

Δy – сума активу Y, яку отримують за торгівлю Δx.

2.6.1 Лінійність функції вартості активу

Спочатку скажемо, що для нашої моделі функція вартості активу *лінійна.*

$$C_{X/Y}(t; \Delta_1 x + \Delta_2 x) = C_{X/Y}(t; \Delta_1 x) + C_{X/Y}(t; \Delta_2 x)$$

Це означає, що кількість активу Y, отримана в результаті одного обміну на деяку кількість активу X, дорівнює кількості активу Y, отриманого під час двох послідовних обмінів, у випадку, коли загалом було обміняно однакову кількість Δx активу X.

Іншими словами, немає різниці як обмінювати одиниці активу, способом (i) або ж (ii), тому що платимо комісію, яка чітко пропорційна обміняному.

Теорема 2.1. ***(лінійність моделі Constant Sum)*** *У наших позначення виконується така невірність:*

$$\Delta y = \Delta_1 y + \Delta_2 y. \tag{2.9}$$

Доведення. Розглянемо два можливі випадки:

(i) обмін всієї кількості Δx на Δy

(ii) обмін первної кількості $\Delta_1 x$ на $\Delta_1 y$, а потім $\Delta_2 x$ на $\Delta_2 y$

У випадку (i), виходячи з рівностей $S = x + y = (x + \gamma\Delta x) + (y - \Delta y)$, отримаємо Δy як

$$\Delta y = \gamma \Delta x$$

У випадку (ii), виходячи з рівностей $S = (x+\gamma\Delta_1 x)+(y-\Delta_1 y)$, після першого обміну отримаємо

$$\Delta_1 y = \gamma \Delta_1 x,$$

а новим продуктом в даному випадку буде

$$S' = x' + y' = (x + \Delta_1 x) + (y - \Delta_1 y) = S,$$

де $S = x + y = (x + \gamma\Delta_1 x) + (y - \Delta_1 y)$ та $\Delta_1 y = \gamma\Delta_1 x$,

То після другого обміну отримуємо

$$\Delta_2 y = \gamma\Delta_2 x,$$

Сумуємо перший та другий обміни, отримуємо:

$$\Delta_1 y + \Delta_2 y = \gamma\Delta_1 x + \gamma\Delta_2 x = \gamma(\Delta_1 x + \Delta_2 x) = \gamma\Delta x$$

Отже,

$$\Delta y = \Delta_1 y + \Delta_2 y = \gamma\Delta x$$

□

2.6.2 Коефіцієнт взаємно обернених свопів

Нехай спочатку в пулі було x одиниць активу X і y одиниць активу Y. Після цього було здійснено два взаємно обернені свопи:

(i) поклали Δx одиниць активу X і взяли з нього відповідну кількість Δy одиниць активу Y.

(ii) одразу ж здійснили зворотну операцію: поставили Δy одиниць активу Y в пул і забрали відповідну суму $\Delta_1 x$ одиниць активу X.

Задача полягає в тому, щоб оцінити втрати від таких повторних обмінів.

Теорема 2.2. ***(втрати при двох взаємно обернених свопах)*** *У наших позначеннях виконується наступна рівність:*

$$\Delta_1 x = \gamma^2 \Delta x \tag{2.10}$$

Доведення. Початкова умова: $S = x + y$

Тоді після першої транзакції (i) отримаємо:

$$\Delta y = \gamma \Delta x$$

Новий продукт буде дорівнювати:

$$S' = x' + y' = (x + \Delta x) + (y - \Delta y)$$

Після другої транзації (ii) ми обчислюємо значення $\Delta_1 x$ з рівності:

$$S' = x' + y' = (x' - \Delta_1 x) + (y' + \gamma \Delta y)$$

Виходить, що

$$\Delta_1 x = \gamma \Delta y = \gamma \cdot \gamma \Delta x = \gamma^2 \Delta x$$

□

Наслідок 2.1. *У даних позначення*

$$C_{Y/X}(t; C_{X/Y}(t,x)) = \gamma^2 x, \tag{2.11}$$

де

$$\mu = \gamma^2. \tag{2.12}$$

Надалі ці твердження будуть використані в наступному розділі для обгрунтування вибору параметрів та умов ліквідації.

2.7 Процес ліквідації позиції для CSM

Оскільки саме цей спосіб закриття позиції несе в собі найбільший ризик, особливу увагу слід приділити його опису та деталізації умов ліквідації позиції. У зв'язку з цим, у цьому розділі буде детально описано процес ліквідації, а потім на основі цього опису встанлено та обґрунтовано *умову ліквідації*, умова, при якій позиція повинна бути негайно закрита (ліквідована).

Примустимо, що позиція була відкрита в момент t_0 (нехай $t_0 = 0$) і змушена закритися в момент часу $t > 0$. Тоді припускаємо, що процес закриття позиції займає майже ненульовий час, що пов'язано з підвищеною затримкою ідентифікації ризикових пропозицій зберігачами і затримкою виконання транзакції в блокчейні. Як бачимо, далі будемо вважати, що цей час з великою ймовірністю обмежений верхньою межею в 10 хвилин. Це завищений факт, але він повністю відповідає нашому наміру зменшити ризики та втрати.

Згідно з даною нотацією, після відкриття позиції Трейдер має y одиниць активу Y, де y залежить від депозиту Трейдера (тобто від типу депозитного активу та від величини депозиту, див.2.3 – 2.5) та від величини кредитного плеча, яку Трейдер обирає в допустимій області. При закритті позиції шляхом ліквідації в деякий момент часу t Зберігач здійснює зворотну операцію, обмінюючи y одиниць активу Y на $x(t)$ одиниць активу X, де

$$x(t) = C_{Y/X}(t,y). \tag{2.13}$$

Зауваження. Комісія за цю транзацію не залежить від значення y, але суттєво залежить від складності транзації. Згідно з протоколом, для проведення транзації Зберігач використовує власні кошти, тому винагорода Зберігача повинна бути досить великою, щоб вважати цю роботу вигідною.

Далі, під час виконання транзакції (проміжок часу між появою умови ліквідації та фактичним включенням транзакції в блокчейн) вартість активу Y може зменшитися відносно активу X. Будемо вважати, що під час виконання транзації (в межах 10 хвилин), максимальна частка падіння активу Y відносно активу X не перевищує певного значення $\nu \in (0,1)$. Очевидно, що значення ν поводяться по-різному для різних активних пар.

Беручи до уваги значення ν, після завершення транзакції отримаємо

найменше

$$(1-\nu)\cdot x(t) \tag{2.14}$$

одиниць активу X.

З цієї суми необхідно здійснити наступні платежі:

– погашення боргу з відром, яке складається з x_0 одиниць активу X;

– комісія за запозичення Трейдера (BF), нарахована за поточною річною ставкою запозичення (BAR), що розраховується за формулою відсотково-складного співвідношення (Кредитори також отримують певні кошти з цієї комісії, залежно від часових інтервалів надання ліквідності та обсягу ліквідності, відповідно до правил протоколу);

– частина Комісії за запозичення Трейдера, яка нараховується протягом періоду ліквідації(з моменту, коли настає умова ліквідації, що спричиняє ліквідацію, і до закінчення процесу ліквідації).

Величина BF Трейдера протягом часового інтервалу t розраховується щосекунди, виходячи з поточного BAR, як складний відсоток від позиченої ліквідності. Величина BAR не є постійною, її значення залежить від так званого *коефіцієнта використання* - частки позикової ліквідності в пулі (чим більший коефіцієнт використання, тим більше значення BAR). Припустимо, що $N = N_t$ - це кількість секунд у часовому інтервалі t , де N_t поділено на m періодів стійкості BAR: $N_t = n_1 + \ldots + n_m$, де n_i - тривалість (в секундах) i-го періоду стійкості; α_i – значення BAR на цьому періоді, поділене на кількість секунд в році; m - кількість періодів. Тоді повна вартість платежів Трейдера за використання x_0 одиниць активу X протягом часу t може бути виражена як

$$\varepsilon(t)\cdot x_0, \tag{2.15}$$

де $\varepsilon(t) = (1+\alpha_1)^{n_1}\cdot\ldots\cdot(1+\alpha_m)^{n_m}$.

Тоді, згідно з нашими припущеннями, період ліквідації обмежений 600 секундами, а максимальне значення BAR становить 1000%. Таким чином, навіть якщо BAR злетить до максимуму під час ліквідаційного

періоду, загальний BF (з моменту відкриття позиції до моменту її закриття) буде не більшим, ніж

$$\Delta \cdot \varepsilon(t) \cdot x_0 = (1.0002 \cdot \varepsilon(t) \cdot x_0 \leqslant (1 + 2 \cdot 10^{-4}) \cdot \varepsilon(t) \cdot x_0, \tag{2.16}$$

де

$$\Delta = (1.0002 \leqslant (1 + 2 \cdot 10^{-4})$$

.

Отже, після завершення ліквідаційної транзакції, отримуємо $(1 - \nu) \cdot x(t)$ одиниць активу X, і не більше $\Delta \cdot \varepsilon(t) \cdot x_0$ одиниць активу X має бути сплачено як BF.

Тому, щоб гарантувати сплату всіх необхідних платежів, слід виконати наступну умову:

$$(1 - \nu) \cdot x(t) \geqslant \Delta \cdot \varepsilon(t) \cdot x_0, \tag{2.17}$$

яку будемо називати **умовою ліквідації**.

Отже, "тригером"для початку ліквідації є момент, коли вперше виконується наступна умова, яка я обернена до 2.17:

$$(1 - \nu) \cdot x(t) \leqslant \Delta \cdot \varepsilon(t) \cdot x_0, \tag{2.18}$$

яку приведемо до такого виду

$$\frac{(1 - \nu) \cdot x(t)}{\Delta \cdot \varepsilon(t) \cdot x_0} \leqslant 1. \tag{2.19}$$

Припустимо, що перед закриттям позиції (в деякий момент часу $t > 0$) Трейдер було y одиниць активу Y. Тоді після закриття позиції, отримана сума активу X дорівнює $x(t) = C_{Y/x}(t,y)$ одиниць.

Аналогічно до виведення нерівності 2.17, можна отримати вираз для вартості $x'(t)$ - кількості одиниць активу X, яка залишиться після здійснення всіх платежів, враховуючи можливе падіння вартості активу

Y та максимальне значення BAR під час закриття позиції:

$$x'(t) = (1 - \nu) \cdot x(t) - \Delta \cdot \varepsilon(t) \cdot x_0 \tag{2.20}$$

2.8 Встановлення максимального допустимого кредитного плеча для відкриття позиції

Спираючись на 2.18, ліквідація позиції має розпочинатися одразу після її відкриття, якщо виконується така умова :

$$(1 - \nu) \cdot x(0) \leqslant \Delta \cdot \varepsilon(0) \cdot x_0 = \Delta \cdot x_0, \tag{2.21}$$

так як $\varepsilon(0) = 1$.

Уникнути такої ситуації можна, задавши правильне значення L_{max} та розглянувши відповідні обгрунтування нище.

2.8.1 Депозитний актив W збігається з позиченим активом Y

В цій роботі розглядаємо випадок, коли актив депозита співпадає з активом Y.

Іншими словами, $Y = W$.

Щоб уникнути негайної ліквідації, потрібно забезпечити умову, протилежну до 2.21:

$$(1 - \nu) \cdot x(0) > \Delta \cdot x_0, \tag{2.22}$$

що є ключовою нерівністю для вибору L_{max}.

У цьому випадку використовується нерівність 2.22. Значення $x(0)$

визначається наступним чином:

$$\begin{aligned} x(0) = C_{Y/X}(0,y + w_0) &= C_{Y/X}(0,C_{X/Y}(0, x_0) + w_0) \\ &= C_{Y/X}(0,C_{X/Y}(0, x_0)) + C_{Y/X}(0, w_0). \end{aligned} \tag{2.23}$$

Використовуючи Теорему2.2, отримуємо:

$$x(0) \geqslant \mu \cdot x_0 + C_{Y/X}(0, w_0). \tag{2.24}$$

Далі, за допомогою 2.24, можна записати нерівність, яка гарантує правильність нерівності 2.22:

$$(1 - \nu)(\mu \cdot x_0 + C_{Y/X}(0, w_0)) > \Delta \cdot x_0.$$

Підставляємо $x_0 = (L - 1) \cdot C_{Y/X}(0, w_0)$ в останню нерівність та отримуємо:

$$(1 - \nu)(\mu \cdot (L - 1) \cdot C_{Y/X}(0, w_0) + C_{Y/X}(0, w_0)) > \Delta \cdot (L - 1) \cdot C_{Y/X}(0, w_0),$$

або ж

$$(1 - \nu)(\mu \cdot (L - 1) + 1) > \Delta \cdot (L - 1). \tag{2.25}$$

Це призводить до обмеження розміру кредитного плеча як

$$L_{max} - 1 < \frac{1 - \nu}{\Delta - \mu \cdot (1 - \nu)}$$

або

$$L_{max} < \frac{\Delta + (1 - \mu) \cdot (1 - \nu)}{\Delta - \mu \cdot (1 - \nu)}. \tag{2.26}$$

Визначимо максимальне плече для пари USDT/USDC.

Проаналізувавши волотильність для пар USDT/USDC та USDC/USDT на сайті *Investing.com* [1], було визначено, що волотильність ніколи за останні 2 роки не перевищувала 5%.

Відповідно розглянуто волотильність $\nu = 0.05$, як для найгіршого випадку.

З нерівності 2.26 видно, що в чисельнику значення $(1 - \mu) \cdot (1 - \nu)$ буде дуже крихітним.

Тому цим значенням можна нехтувати. А отже, виходить нова формула для розрахунку максимального плеча:

$$L_{max} < \frac{\Delta}{\Delta - \mu \cdot (1 - \nu)}. \tag{2.27}$$

Враховуючи, що $\mu = 0.994$ з Наслідку2.1 та $\nu = 0.05$

Отримуємо

$$L_{max} < \frac{1.0002}{1.0002 - 0.994 \cdot (1 - 0.05)} < 17.37. \tag{2.28}$$

Виходить, що максимальне плече дорівнює

$$L_{max} = 17. \tag{2.29}$$

Таким чином, для будь-якого пула, коли Трейдер бере один з стейблкоїнів та обмінює на інших стейблкоїн, то підходить плече 17, тому що волотильність обмежена 5%.

Приклад 2.2. Трейдер бере 100 USDT і хоче обміняти на USDC. Тому що вірить, що USDC буде зростати відносно USDT.

Трейдеру кажуть, що йому можуть дати на цю пару 17 плече.

Тобто, якщо в нього було 100 USDT, то він може взяти же 1600 USDT, щоб в сумі було $17 \cdot 100 = 1700$ USDT.

Потім Трейдер бере свої 100 USDT та ще 1600, і це все переводить в USDC.

І далі чекає поки USDC почне рости.

Отже, максимальне кредитне плече використовують для того, аби збільшити потенційний прибуток.

Основна ціль Трейдера – вірно передбачити зміну цін та ринку та збільшити в рази свої активи. В прикладі, розглянутому вище, Трейдер має змогу збільшити свій прибуток потенційно в 17 разів порівняно з інвестицією без використання плеча.

Але Трейдеру потрібно чітко усвідомлювати та аналізувати всі можливі ризики, оскільки він може неправильно передбачити зміну цін і понести втрати в тому ж співвідношенні, що й можливий прибуток.

Висновки до розділу 2

В цьому розділі було описано основні типо DeFi протоколів, зокрема детальніше розглянуто протокол Constant Sum, який є одним із протоколів AMM. Були приведені аргументи актуальності та важливості даної теми роботи. Було формалізовано математичну модель цього протоколу, а саме, вперше була наведена явна формула, яка повністю описує процес децентралізованого обміну активів згідно до протоколу Constant Sum. Також вперше було формульовано і доведено дві основні властивості цієї моделі, від яких залежать параметри маржинальної торгівлі, це властивість лінійності та властивість втрат при подвійній транзакції. Було описано різні випадки трейдингу в залежності від стану коштів. Власне все, що може знадобитись для розуміння основної постановки задачі цієї роботи. Далі була виведена загальна формула для встановлення максимального допустимого кредитного плеча, згідно цього проведено аналіз та зроблено висновок, що дана модель відходить для пар стейблкоїнів. Проведено математичне дослідження окремого випадку та для нього виведена формула для максимального плеча.

ВИСНОВКИ

У наведеній роботі було проведено аналіз та обгрунтування властивостей DeFi моделі Constant Sum для вибору параметрів протоколу маржинальної торгівлі. У ході даної роботи було розглянуто переваги та недоліки технонології блокчейн та описано основні типи DeFi протоколів. Було описано процес роботи моделі Constant Sum, доведено лінійність цієї моделі, описано умови ліквідації. Завершальним етапом було обгрунтувано процес вибору максимального допустимого кредитного плеча для відкриття позиції та вивід загальної формули як для цієї моделі вцілому, та й для окремого випадку.

Модель Constant Sum раніше існувала виключно теоретично, що могло призводити до нестабільності ринку, зловживання або незрозумілих ситуацій, що негативно впливали на довіру до блокчейн-мереж та розвиток цифрових активів і тд. В цій роботі було вперше запропоновано математичне обгрунтування методу вибору максимального допустимого кредитного плеча та умови ліквідації для вказаної моделі. Отримані формули дозволили проаналізувати модель та на основі цього зробити висновок, що така модель найбільше підходить для пар стейблкоінів, тому було прораховано саме максимальне кредитне плече для таких пар. Для пар стейблкоінів плече вийшло досить велике (до 17), у порівнянні з більш волотильними активами, де плече 4-6.

Дані математичні обгрунтування дозволяють підвищити ефективність торгівлі та зменшити ризики нерівноважності ринку, що можуть призвести до недооцінки ризиків або використання неоптимальних стратегій маркет-мейкінгу.

Для вирішення проблеми дефіциту чіткого математичного обгрунтування в цій сфері потрібно проводити більше досліджень та розробок в галузі блокчейн-маркет-мейкінгу, що базуються на математичних моделях та алгоритмах. Це допоможе створити стабільніші

та надійніші блокчейн-ринки, де маркет-мейкери зможуть ефективно функціонувати та забезпечувати ліквідність.

Одним з напрямків подальших досліджень може бути застосування цього математичного апарату не тільки для маржинальної торгівлі, а і для залогової торгівлі.

ПЕРЕЛІК ПОСИЛАНЬ

[1] URL: https://www.investing.com/.

[2] H. Adams та ін. *Uniswap v3 Core*. Англ. 2021. URL: https://uniswap.org/whitepaper-v3.pdf.

[3] S. Coelho-Prabhu. *A Beginner's Guide to Decentralized Finance (DeFi)*. Англ. 2020. URL: https://www.coinbase.com/blog/a-beginners-guide-to-decentralized-finance-defi.

[4] Coinbase. *What is a DEX?* Англ. 2021. URL: https://www.coinbase.com/ru/learn/crypto-basics/what-is-a-dex.

[5] D. Krupka. *Aave (LEND) Review: Decentralised Lending Platform*. Англ. 2021. URL: https://www.coinbureau.com/review/aave-lend/.

[6] S. Onyshchenko. *AMM TYPES DIFFERENTIATIONS*. Англ. 2020. URL: https://blaize.tech/article-type/amm-types-differentiations/.

[7] A. Port та N. Tiruviluamala. *Mixing Constant Sum and Constant Product Market Makers*. Англ. 2022. URL: https://arxiv.org/pdf/2203.12123.pdf.

[8] R. Schulpen. *Smart contracts in the Netherlands A legal research regarding the use of smart contracts within Dutch contract law and legal framework*. Англ. 2018. URL: http://arno.uvt.nl/show.cgi?fid=146860.

[9] N. Tang. *What is an Automated Market Maker?* Англ. 2020. URL: https://phemex.com/academy/what-is-an-automated-market-maker-amm.

[10] N. Tang. *What is Chainlink (LINK)? How Oracles Connect Blockchain Data to the Real World*. Англ. 2022. URL: https://phemex.com/academy/what-is-chainlink-link.

[11] *What Are Automated Market Makers (AMMs)?* Англ. 2022. URL: https://chain.link/education-hub/what-is-an-automated-market-maker-amm.

[12] *Что такое Aave?* Рос. 2021. URL: https://forklog.com/cryptorium/chto-takoe-aave.