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

«На правах рукопису»
УДК 336.764/.768

«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: **«Вибір параметрів DeFi протоколу, що базується на моделі Constant Product Market»**

Виконав:
студент IV курсу, групи ФІ-94
Коробан Ольга Михайлівна _____

Керівник:
д.т.н., професор кафедри ММЗІ
Ковальчук Людмила Василівна _____

Рецензент:
посада, степінь, звання
Прізвище Ім'я По-батькові _____

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

Студент _____

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

Студент: Коробан Ольга Михайлівна

1. Тема роботи: «*Вибір параметрів DeFi протоколу,*

що базується на моделі Constant Product Market», науковий керівник дисертації: д.т.н., професор кафедри ММЗІ Ковальчук Людмила Василівна,

затверджені наказом по університету №__ від «__» _____ 2023 р.

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

3. Об'єкт дослідження: *DeFI модель Constant Product Market для вибору параметрів протоколу маржинальної торгівлі.*

4. Предмет дослідження: *аналізування властивостей DeFI моделі Constant Product Market та обґрунтування вибору параметрів протоколу маржинальної торгівлі.*

5. Перелік завдань:

– *аналіз процесу обміну двох активів у рамках моделі Constant Product Market*

– *розгляд двох випадків обміну: одна транзакція, сумма розбита на дві транзакції*

– *дослідження нижної і верхньої межі для обох випадків обміну .*

– *опрацювання умов ліквідації транзакції*

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	Огляд опублікованих джерел за тематикою дослідження	Вересень-жовтень 2022 р.	Виконано
3	Дослідження моделі Constant Product Market	Жовтень-листопад 2022 р.	Виконано
4	Аналіз процесів обміну	Грудень -січень 2022 р.	Виконано
5	Дослідження межей обміну	Лютий-квітень 2022 р.	Виконано
6	Опрацювання умов ліквідації транзакції	Травень - 12 червня 2022 р.	Виконано

Студент _____ Ольга Коробан

Керівник _____ Людмила Ковальчук

РЕФЕРАТ

Кваліфікаційна робота містить: 43 стор., 0 рисунки, 0 таблиць, 10 джерел.

Дана робота присвячена обґрунтуванню вибору параметрів для протоколу маржинальної торгівлі. Дослідження зосереджене на аналізі властивостей DeFI протоколу, що базується на моделі Constant Product Market, а також на обґрунтуванні вибору оптимального рівня кредитного плеча.

Об'єкт дослідження є DeFI протокол, що базуеться на моделі Constant Product Market. Предмет дослідження є аналіз властивостей DeFI протоколу маржинальної торгівлі та обґрунтування вибору максимально допустимого кредитного плеча.

В рамках цього дослідження був проведений аналіз DeFI протоколу, що базується на моделі Constant Product Market. Визначено межі значень активів після здійснення обміну та перевірили лінійність моделі Constant Product Market. Крім того, визначино умови, за яких може відбутися ліквідація транзакції, та проаналізувано вибір максимально допустимого рівня кредитного плеча.

Практична цінність нашого дослідження полягає у забезпеченні стабільності та продуктивності протоколу маржинальної торгівлі.

БЛОКЧЕЙН ТЕХНОЛОГІЯ, ПРОТОКОЛИ МАРЖИНАЛЬНОЇ ТОРГІВЛІ, МОДЕЛЬ CONSTANT PRODUCT, МАКСИМАЛЬНО ДОПУСТИМЕ КРЕДИТНЕ ПЛЕЧЕ

ABSTRACT

The qualification work contains: 43 pages, 0 figures, 0 tables, 10 references.

This work is dedicated to justifying the choice of parameters for the margin trading protocol. The research focuses on analyzing the properties of the DeFI protocol based on the Constant Product Market model and justifying the selection of the optimal level of leverage.

The object of the research is the DeFI protocol based on the Constant Product Market model. The subject of the study is the analysis of the properties of the DeFI margin trading protocol and the justification of the choice of the maximum allowable leverage.

Within this research, an analysis of the DeFI protocol based on the Constant Product Market model was conducted. The limits of asset values after the exchange were determined, and the linearity of the Constant Product Market model was verified. Additionally, conditions for transaction liquidation were identified, and the choice of the maximum allowable level of leverage was analyzed.

The practical value of our research lies in ensuring stability and performance of the margin trading protocol.

BLOCKCHAIN TECHNOLOGY, MARGIN TRADING PROTOCOLS, CONSTANT PRODUCT MODEL, MAXIMUM ALLOWABLE LEVERAGE

ЗМІСТ

ВСТУП

Актуальність дослідження. В наш час фінансові ринки стають дедалі складнішими та вимагають багатьох знань та вмінь від інвесторів. Особливо якщо мова йде про криптовалюту. Саме через це з'являються нові інструменти, моделі та методи що допомагають полегшити торгівлю та надають ефективні засоби керування активами. Один з найбільш значущих інструментів на фінансовому ринку стала маржинальна торгівля.

З метою поліпшення даного способу торгівлі виникла необхідність у створенні протоколів та моделей які дозволяють зручно, безпечно та єфективно вибирати параметри для оптимального управління активами.

Ця робота присвячена аналізу та обґрунтування властивостей DeFi моделі Constant Product для вибору параметрів протоколу маржинальної торгівлі. Дослідження спрямоване на виявлення переваг та недоліків даноїмоделі, її ефективності та придатності для використання на фінансових ринках.

Метою дослідженняє детальний аналіз зв'язків між параметрами протоколу та ризиками для нього, а також впливу параметрів на функціональність та ефективність моделі. Для досягнення мети необхідно розв'язати такі**задачі дослідження**:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) Дослідити модель Constant Product Market ;

3) Ретельно проаналізувати процес обміну;

4) Дослідити межі обміну.

5) Визначити умови ліквідації транзакції

Об'єктом дослідження є DeFI модель Constant Product Market для вибору параметрів протоколу маржинальної торгівлі..

Предметом дослідження є вивченні впливу різних параметрів на ефективність і стабільність DeFi протоколу, що базується на моделі Constant Product Market. Такі параметри, як початковий розподіл

активів, комісії, граничні значення для торгівлі і механізми збереження ліквідності.

Наукова новизна дослідження полягає в розробці методології для вибору оптимальних параметрів DeFi протоколу, що базується на моделі Constant Product Market, з метою забезпечення ефективності та стабільності функціонування протоколу.

Практичне значення даної роботи полягає в тому, що вибір оптимальних параметрів DeFi протоколу, що базується на моделі Constant Product Market, дозволяє забезпечити оптимальне розподілення ліквідності та максимізувати вигоди для користувачів протоколу. Це може сприяти зниженню ризиків та підвищенню ефективності фінансових операцій, здійснюваних у межах протоколу.

1 БЛОКЧЕЙН ТЕХНОЛОГІЯ

У цьому розділі ми опишемо що таке блокчейн, його застосування, актуальність та принципи роботи технологій пов'язаних з ним.

1.1 Створення блокчейн

Блокчейн вперше став відомим зі з'явленням Bitcoin, коли Сатоші Накамото опублікував технічну документацію в 2009 році. Неможливо виділити одного винахідника блокчейну, однак походження технології блокчейн можна прослідкувати до 1991 року, коли фізик Стюарт Хабер і криптограф В. Скотт Сторнетта опублікували дослідницьку статтю під назвою "Як забезпечити часовий штамп для цифрового документа".

У дослідницькій статті розглядалася незмінність цифрових записів за допомогою Time Stamping Service(TSS), що використовує хеш-функції та цифрові підписи для перевірки оригінальності конкретного документа. Документи пов'язуються між собою, утворюючи послідовність часу для перевірки часових штампів, пов'язаних з кожним документом. Ця послідовність документів була найпростішою версією блокчейну, яку пізніше використав Нік Сзабо у Bit Gold, ранньому варіанті цифрової валюти.

1998 року, відомий комп'ютерний вчений Нік Сзабо почав працювати над ідеєю децентралізованої валюти, яку він назвав "Bit Gold". Він опублікував технічну документацію, в якій запропонував ланцюг хешів з часовим штампом (блокчейн), який може вирішити проблему подвійного витрачання за допомогою hashcash - ранньої версії системи Proof-of-Work для обмеження спаму на форумах та електронній пошті.

Bit Gold вперше представив концепцію вартості на основі витрат

обчислювальних ресурсів. Вартість "бітів"розраховується на основі складного математичного рівняння. Усі "біти"зберігаються в блокчейні разом із їхньою вартістю, яка корелює з витратами на їх обчислення.

Ідея Bit Gold не матеріалізувалася, оскільки Нік Сзабо не був впевнений у її реалізації. Найбільшою недоліком Bit Gold було взаємозв'язання між вартістю та витратами на обчислення. У Bitcoin Сатоші Накамото відокремив вартість від витрат на обчислення, а вартість визначається на відкритому ринку.

Якщо вартість безпосередньо корелює з витратами на обчислення, це може створити непослідовності в мережі, оскільки одна монета матиме вищу вартість, ніж інша лише через витрати на обчислення. У випадку Bitcoin вартість одного добутого Bitcoin у 2010 році має таку ж вартість, як і Bitcoin, добуті сьогодні. Якщо б вартість Bitcoin була пов'язана з витратами на обчислення, то всі Bitcoin, добуті у 2010 році, були б значно дешевшими, ніж Bitcoin, які добуваються сьогодні, оскільки витрати на добуток Bitcoin у 2010 році були значно нижчими.

У 2000 році Стефан Конст запропонував ідею криптографічно захищених ланцюгів у дослідній статті під назвою "Захищені журнали на основі криптографічно з'єднаних записів". Він представив модель, в якій записи у ланцюгу можуть бути прослідковані від генезису для підтвердження автентичності - цю саму модель ми бачимо в Bitcoin та інших криптовалютах сьогодні. У 2008-2009 роках Сатоші Накамото випустив технічну документацію Bitcoin, об'єднавши всі ідеї розподіленого реєстру разом з безпечними криптографічними функціями, презентуючи практичне застосування блокчейну. Після, блокчейн-технологія продовжувала активно розвиватися. Відкрився шлях до створення нових криптовалют, які базуються на технології блокчейн.

У 2013 році Віталік Бутерин представив Ethereum - платформу для розробки децентралізованих додатків. Ethereum вперше впровадив поняття смарт-контрактів, що дозволяють виконувати автоматичні операції без посередництва. Це значно розширило можливості

блокчейн-технології, дозволяючи створювати різноманітні децентралізовані додатки та платформи.

У 2015 році група розробників випустила протокол блокчейн під назвою Hyperledger Fabric. Цей протокол спрямований на застосування блокчейн-технології в корпоративному середовищі, забезпечуючи конфіденційність, масштабованість та гнучкість. Hyperledger Fabric став основою для створення різноманітних блокчейн-рішень для бізнесу та фінансових установ.

Одним із важливих етапів розвитку блокчейн-технології було появлення концепції приватних блокчейнів. У таких блокчейнах доступ до записів та участь в мережі регулюється дозволами, що дозволяє досягти більшої конфіденційності та контролю. Багато компаній та фінансових установ використовують приватні блокчейни для покращення ефективності своїх операцій та забезпечення безпеки даних.

З поступом часу блокчейн-технологія стала застосовуватися в різних галузях, включаючи логістику, медицину, нерухомість, голосування та багато інших. Вона надає можливість забезпечити безпеку, достовірність та прозорість обміну даними та транзакціями між учасниками мережі.

Сьогодні блокчейн-технологія продовжує еволюціонувати, з'являються нові інновації та використання. Це свідчить про потужний потенціал блокчейну як технології, що може перетворити багато галузей життя та забезпечити нові можливості для ефективностіта безпеки .

1.2 Що таке технологія блокчейн?

Щоб описати поняття блокчейн розглянемо його як цифрову систему, що базується на принципах бухгалтерської книги, в якій зберігаються та реєструються транзакції. Кожен раз, коли гроші переказуються з одного рахунку на інший, ці операції записуються в бухгалтерську книгу, що доступна загальному огляду.

Блокчейн, в свою чергу, представляє собою цифрову версію цієї "бухгалтерської книги доступну для широкої громадськості.

Термін "блокчейн"походить від способу функціонування цих цифрових реєстрів.

Блокчейн - це цифрова книга, що реєструє інформацію таким чином, що учасникам важко змінити або обдурити систему.

Використовуючи криптовалюти як приклад, як тільки транзакція починається у мережі, вона додається до "блоку"разом з іншими аналогічними транзакціями. Блок - це структура даних, що постійно зберігає інформацію про транзакції у блокчейні.

Після цього група перевіряючих виконує перевірку цього блоку за допомогою процесу, відомого як майнінг блокчейну, для гарантування відсутності шахрайства або дублікатів. Після завершення цієї перевірки, перевіряючі "прикріплюють"цей блок транзакцій до інших блоків у мережі, створюючи блочний шар.

Технологія блокчейн має деякі ключові особливості. Перша з них - це розподілений реєстр, який гарантує єдиний запис транзакцій. Це усуває необхідність дублювання зусиль, яке часто зустрічається в звичайних бізнес-процесах.

Друга особливість - незмінність. Блокчейн за своєю природою є незмінною базою даних. Дані, що зберігаються в мережі блокчейн, є постійними. Вони не можуть бути змінені, фальсифіковані або маніпульовані.

Ще одна особливість полягає в тому, що транзакції блокчейна є незмінними записами, що означає, що вони захищені від несанкціонованого доступу і можуть бути завантажені лише один раз. Це ускладнює підробку історії транзакцій організацією.

Найголовніше, технологія блокчейн використовує дуже смарт-контракти для прискорення процесів та підвищення ефективності. Ці автоматичні коди слідують визначеним параметрам і метрикам при перевірці транзакцій та достовірності інформації, доданої до блокчейну.

Основна ідея, що підштовхує до спонтанного зростання технології блокчейн, полягає у її децентралізованому характері. Таким чином, передача вартості та активів здійснюється на основі "користувач-до-користувача"або "peer-to-peer "(P2P) мережі. Ця функція усуває посередників, таких як визнані фінансові установи, які часто втручаються в бізнес-процеси.

Замість цього користувачі можуть здійснювати транзакції між собою, тим самим економлячи банківські витрати, позбавляючись фіктивної складності та прискорюючи процес виконання бізнесу.

На практиці всі типи блокчейнів працюють однаково. Вони ґрунтуються на майнерах, які перевіряють блоки транзакцій і додають їх до блокчейнів окремо. Ці майнери працюють з складним апаратним і програмним забезпеченням, і їхня робота має вирішальне значення для функціональності блокчейну.

Транзакції записуються у вигляді блоків даних. Зазвичай ці дані містять короткий опис транзакції. Наприклад, у випадку криптовалютних транзакцій, вони часто включають інформацію про залучені сторони, суму транзакції і т. д.

Валідатор додає новий блок до існуючого блоку в мережі, утворюючи ланцюжок. Як тільки цей ланцюжок сформований, стає неможливим змінювати або додавати нові блоки між ними.

Кожен новий блок автоматично перевіряє автентичність попереднього, що призводить до рівня довіри, якого часто бракує у звичайному фінансовому просторі.

Ця архітектура робить ланцюжок блоків незмінним або непіддаємим змінам для зовнішніх суб'єктів.

Існують три популярних типи блокчейн-мереж:

1) Публічні блокчейн-мережі:

Більшість криптопротоколів, таких як Bitcoin і блокчейн EOS, відносяться до цієї категорії. Ці проекти мають відкритий вихідний код, що означає, що кожен може легко використовувати їх і відстежувати

транзакції в мережі через переглядач блокчейна. Блокчейни, такі як Bitcoin, використовують алгоритм консенсусу Proof-of-Work (PoW). Алгоритм PoW передбачає, що валідатори змагаються у вирішенні складних математичних завдань, що забезпечує великий рівень безпеки за рахунок швидкості, енергоефективності та вартості. Через цю функцію мережа Bitcoin часто критикується за енергозатратний процес перевірки. Хоча це залишається ключовою проблемою для мережі Bitcoin, деякі публічні блокчейни вже перейшли на більш енергоефективну та економічну модель консенсусу, відому як Proof-of-Stake (PoS). У моделі PoS власники криптовалюти можуть ставити свої монети та створювати вузли-валідатори для перевірки транзакцій у мережі.

2) Приватні блокчейн-мережі:

Приватна мережа блокчейн допускає лише обмежену кількість учасників. Учасники можуть приєднатися до таких мереж лише за автентичними та перевіреними запрошеннями. Таким чином, приватний блокчейн контролює, хто може брати участь у мережі, виконувати протоколи консенсусу та підтримувати спільний реєстр. Власники цих блокчейнів мають право редагувати, переозначати та видаляти будь-які записи в блокчейні на свій розсуд. Hyperledger - приклад приватної блокчейн-мережі. Приватні блокчейни були критиковані за їх недостатню децентралізацію. Вони представляють закриті безпечні бази даних, що надають доступ лише обмеженому колу учасників для запуску вузлів, здійснення транзакцій або перевірки автентичності налаштувань.

3) Дозволена мережа блокчейнів:

Блокчейн з дозволами працює як комбінація приватних та публічних блокчейнів. Ці блокчейни підтримують кілька точок зору на налаштування, включаючи можливість приєднання будь-якого після достатньої перевірки його особистості. Головна ідея дозволеного блокчейна полягає в тому, щоб надавати спеціальні дозволи кожному учаснику, щоб вони могли виконувати певні функції та обробляти певні процеси. Обмежуючи певні функції, дозволені блокчейни можуть бути

відкриті для більшої кількості людей.

1.3 Переваги блокчейн

Безпека: Його розподілена архітектура на основі консенсусу усуває одні точки відмови та зменшує потребу у посередниках даних, таких як агенти переказу, оператори систем повідомлень та неефективні монополістичні комунальні служби. Ethereum також дозволяє впровадження безпечного програмного коду, призначеного для запобігання шахрайству та зловживанню з боку зловмисних третіх осіб, що майже неможливо зламати або зманіпулювати.

Прозорість: Він використовує узгоджені стандарти, протоколи та спільні процеси, виступаючи як єдине джерело правди для учасників мережі.

Довіра: Його прозорий та неухильний реєстр сприяє зручному співробітництву різних сторін у бізнес-мережі, керуванню даними та досягненню угод.

Програмованість: Він підтримує створення та виконання розумних контрактів - незмінних програм, які автоматизують бізнес-логіку, що забезпечує збільшену довіру та ефективність.

Приватність: Він надає передові інструменти для гранульованої конфіденційності даних на всіх рівнях програмного стеку, дозволяючи селективне обмінювання даними в бізнес-мережах. Це значно покращує прозорість, довіру та ефективність, зберігаючи приватність та конфіденційність.

Висока продуктивність: Його приватні та гібридні мережі розроблені для підтримки сотень транзакцій на секунду та періодичних скачків активності мережі.

Масштабованість: Він підтримує здатність взаємодіяти між приватними та публічними ланцюжками, надаючи кожному підприємницькому рішенню глобальний охоплення, велику стійкість та

високу надійність основної мережі.

1.4 Основні поняття технології протоколу блокчейн

Proof of Work протокол є невеликим рядком даних, створення якого складне для комп'ютера, але легко перевіряється зовнішніми сторонами. Докази роботи є тим, що ускладнює процес майнінгу біткоїну, дозволяючи при цьому кому завгодно довести, що нові монети були створені законно.

Розподілений реєстр - це публічно видима історія транзакцій, яку може побачити будь-хто у більшості проектів криптовалют.

Smart Contracts базуються на системі доказу роботи, яку створив біткоїн, для укладання і створення безпечних контрактів. Ідея розумних контрактів полягає в тому, щоб сприяти більш ефективній цифровій комерції, дозволяючи сторонам укладати контракти програмно за долю секунди.

Монети і токени Переміщення монет між гаманцями потребує технічних знань і створює ризики безпеки для користувачів, які не є експертами в протоколах блокчейн. Фізичне переміщення монет також може створювати проблеми з регулюванням. Тому більшість блокчейн-сервісів, таких як криптовалютні біржі та торгові платформи, використовують токени для передачі значення між користувачами. У системах на основі токенів постачальник володіє значною кількістю монет, а власність цих монет передається між користувачами під час транзакцій. Токени можуть полегшити транзакції, але проблема полягає в тому, що реальна власність залишається у постачальника, а не у окремих користувачів.

1.5 Протоколи блокчейну

1) **Hyperledger**

Hyperledger - це проект з відкритим кодом, який має на меті створити набір інструментів для підприємств, щоб швидко та ефективно впроваджувати технології блокчейну. Протокол часто використовується в рішеннях програмного забезпечення блокчейну, оскільки він має свої бібліотеки, які допомагають прискорити розробку. Linux Foundation є сильним прихильником Hyperledger і надає значний досвід для прискорення створення протоколу. Hyperledger також добре сумісний з Linux, тому він розроблений для ефективної роботи на тих же серверах, що широко використовуються в сучасному бізнес-світі.

2) **Multichain**

Multichain був створений для допомоги комерційним корпораціям у створенні приватних блокчейнів для полегшення більш ефективних транзакцій та розробки нових додатків для систем proof-of-work, на яких ґрунтуються технології блокчейну. Як приватна компанія, Multichain може надати API, який може використовуватися службами розробки блокчейну для спрощення інтеграції та прискорення впровадження. Те, що відрізняє Multichain від його конкурентів, полягає в тому, що він розроблений для використання разом з фіатними валютами та фізичними засобами збереження вартості. У порівнянні з більшістю криптовалютних проектів, які спрямовані на остаточну заміну фізичних грошей цифровими засобами обміну.

3) **Enterprise Ethereum**

Ethereum пропонує версію свого програмного забезпечення, яке розроблено для використання в бізнес-сценаріях. Метою Ethereum Enterprise є збільшення бізнес-сценаріїв розробки програмного забезпечення блокчейну. За допомогою Ethereum Enterprise підприємства можуть швидко розробляти масштабні додатки для обміну значення. Основною перевагою Ethereum Enterprise є те, що воно дозволяє підприємствам створювати власні варіанти Ethereum, при цьому повністю використовуючи останній код Ethereum. У звичайних умовах ліцензія Ethereum ускладнює створення власних варіантів програмного

забезпечення, але підприємницька версія дає підприємствам можливість обійти це обмеження.

4) **Corda**

Corda є конкурентом Multichain і пропонує протокол, призначений для підприємств. Більшість додатків, які були розроблені з використанням Corda, належать до фінансової та банківської сфери. Однак широкий спектр користувальницьких рішень блокчейну може використовувати технологію Corda. Corda має акредитацію від банківського консорціуму R3, тому це гарний вибір для розробки рішень блокчейну в фінансовій галузі.

5) **Quorum**

Так само, як і багато провідних протоколів, Quorum має на меті допомогти бізнесу у фінансовому секторі. Quorum важливий тим, що він має сильну підтримку фінансової спільноти. Наприклад, J.P. Morgan Chase є основним фінансовим спонсором протоколу, і він отримав додаткові ресурси від інших провідних банків. Однак Quorum вдалося залишитися проектом з відкритим кодом, який може використовуватися кожним. Quorum також тісно пов'язаний з Ethereum, оскільки проект почався зі зміни коду Ethereum.

1.6 Automated Market Maker

Автоматизований ринковий мейкер (AMM) - це система, яка автоматично здійснює купівлю та продаж замовлень на децентралізованій біржі. У відміну від звичайних ринкових мейкерів, AMM функціонують за допомогою самовиконуючих комп'ютерних програм, які також відомі як смарт-контракти. Ці смарт-контракти автоматично вирішують операції між покупцями та продавцями.

Використання AMM також усуває необхідність участі іншої сторони при здійсненні угоди. Замість цього, покупці та продавці можуть торгувати безпосередньо з AMM та його алгоритмом, який визначає ціну

криптовалюти, яку ви бажаєте торгувати.

AMM надає можливість торгувати будь-якою криптовалютою без необхідності взаємодії безпосередньо з іншим покупцем або продавцем. На відміну від цього, централізовані криптобіржі, такі як Coinbase або Binance, не використовують AMM. Проте, хоча AMM автоматизують процес транзакцій, все ж потрібні постачальники ліквідності для їхньої роботи.

Пулі ліквідності та постачальники ліквідності

Автоматизовані ринкові мейкери покладаються на пулі ліквідності та постачальників ліквідності для своєї роботи. Пул ліквідності - це резерв криптовалюти, який використовується для здійснення майбутніх угод. Ті, хто надають свої кошти в ці пули, називаються постачальниками ліквідності.

Зазвичай пули ліквідності використовують лише дві криптовалюти, які обмінюються між собою. Наприклад, трейдер може продати Bitcoin (BTC) для купівлі Ether (ETH) та навпаки з пулу ліквідності BTC/ETH за допомогою AMM. Деякі пули ліквідності та AMM обробляють кілька криптовалют одночасно. Це залежить від вашого AMM та децентралізованої біржі.

Принцип роботи Automated Market Maker

Автоматизовані ринкові мейкери покладаються на математичні формули для автоматичного встановлення цін на активи без втручання людини. Пулі ліквідності відіграють ще одну важливу роль у цьому процесі.

На криптобіржі один пул ліквідності містить велику кількість активів, заблокованих у смарт-контракті. Основна мета цих заблокованих токенів - забезпечення ліквідності, отже, сама назва. Для функціонування пулів ліквідності необхідні постачальники ліквідності (тобто постачальники активів), щоб створити ринок.

Ці пули ліквідності можуть використовуватись для різних цілей, таких як фармінг доходу та позичання або кредитування.

У межах пулів ліквідності два різних активи об'єднуються, щоб утворити торгову пару. Наприклад, якщо ви бачите два назви активів поруч, розділені косою рискою (наприклад, USDT/BNB, ETH/DAI) на децентралізованій біржі, то ви дивитесь на торгову пару. У цих прикладах пари - це токени ERC-20 на блокчейні Ethereum (як і більшість децентралізованих бірж).

Співвідношення кількості одного активу до іншого в торговій парі може бути різним. Наприклад, пул може містити 80

Будь-хто може стати ринковим мейкером, внесши заздалегідь встановлене співвідношення двох активів у торгову пару в пул ліквідності. Трейдери можуть торгувати активами проти пулу ліквідності, а не безпосередньо один з одним.

Різні децентралізовані біржі можуть використовувати різні формули AMM. Формула AMM Uniswap використовує досить просту формулу, але вона все одно дуже успішна. У найпростішій формі ця формула виглядає як "x * y = k". У цій формулі "x це кількість першого активу у пулі ліквідності і торговій парі, а "y кількість іншого активу у тому ж пулі і парі.

За допомогою цієї формули будь-який пул, який використовує AMM, повинен підтримувати постійну загальну ліквідність, що означає, що "k"у цьому рівнянні є постійною.

Переваги Automated Market Maker

AMM може усунути посередника і зробити торгівлю на децентралізованих біржах повністю довіреною, що є цінною складовою для багатьох власників криптовалют.

AMM також надають користувачам стимул для надання ліквідності в пулах. Якщо особа надає пулу ліквідності свої активи, вона може заробляти пасивний дохід у вигляді комісій за транзакції інших користувачів. Це фінансовий привабливий елемент, завдяки якому постачальники ліквідності на децентралізованих біржах настільки численні.

Таким чином, AMM відповідають за приведення ліквідності на біржу,

що є їх головною задачею. Тому на DEX-біржах AMM мають вирішальне значення.

Крім того, постачальники ліквідності також можуть отримувати вигоду від фармінгу доходу за допомогою AMM та пулів ліквідності. Фармінг доходу передбачає використання криптовалюти для отримання активів пулу ліквідності в обмін на надання ліквідності. Постачальники також можуть переміщувати свої активи між пулами для максимізації прибутку. Цей прибуток зазвичай представлений у вигляді річної процентної ставки (APY).

Недоліки Automated Market Maker

Недоліком AMM є ситуація, коли є розбіжність між передбачуваною ціною замовлення і ціною, за якою воно фактично виконується. Це можна пом'якшити, збільшуючи обсяг ліквідності відповідного пулу.

Крім цього, AMM та пули ліквідності також пов'язані з так званими втратами через нестійкість. Це втрати коштів, які виникають через коливання цін в торговій парі. Ці коливання відносяться до ціни одного або обох активів у парі. Якщо вартість активів при знятті коштів нижча, ніж була при їх зарахуванні, то власник зазнає втрати через нестійкість.

Нестійкість є поширеною проблемою на децентралізованих біржах, оскільки криптовалюти є волатильними та непередбачуваними за своєю природою. Однак у деяких випадках актив може відновити свою ціну після спаду, тому цей вид втрат відомий як "нестійкі".

1.7 Uniswap

Constant Product Market (CPM) використовується в мережах децентралізованих фінансів (DeFi) для створення та керування ліквідністю торгових пар. Один із найпопулярніших прикладів CPM є протокол Uniswap, який ґрунтується на Ethereum.

Uniswap - це децентралізована біржа, яка дозволяє здійснювати роботу з ринком peer-to-peer. Uniswap також є криптовалютою,

позначеною як (UNI). Платформа Uniswap дозволяє користувачам торгувати криптовалютами без участі централізованої третьої сторони.

Блокчейн Uniswap розміщений на платформі Ethereum та керується власниками UNI. Uniswap описує свій блокчейн як громадський ресурс. Блокчейн Uniswap є відкритим джерелом, що означає, що кожен може переглядати та вносити свій внесок у код блокчейну.

Uniswap — це автоматизований протокол ліквідності. Він не використовує order book або централізованої платформи. Завдяки вбудованим контрактам, Uniswap дозволяє користувачам торгувати без посередників, забезпечуючи високий рівень децентралізації та стійкості до цензури.

Uniswap розробив протокол, який ґрунтується на постачальниках ліквідності, які створюють пули ліквідності. Ці пули забезпечують ліквідність на платформі, дозволяючи користувачам вільно обмінюватися майже будь-якими токенами ERC-20 без потреби у order book.

Оскільки протокол Uniswap повністю децентралізований, тут немає реального процесу лістингу, як на централізованій біржі. Будь-який токен ERC-20 може бути запущений для торгівлі на платформі Uniswap за наявності доступного пула ліквідності. Тому Uniswap не стягує комісію за лістинг, що робить його важливим ресурсом для нових або малих проектів ERC-20.

Uniswap відмовляється від традиційної архітектури цифрових централізованих бірж і залишає в минулому order book. Це стало можливим, відчасти, завдяки їх дизайну постійного маркет-мейкера, який є варіацією більш поширеної моделі децентралізованого обміну, відомої як автоматизований маркет-мейкер (AMM).

Автоматизовані маркет-мейкери - це смарт-контракти, які містять резерви ліквідності (пули), якими можуть користуватися трейдери для торгівлі. Ці резерви фінансуються зацікавленими постачальниками ліквідності. Будь-хто, хто може внести еквівалентну вартість двох різних токенів в пул, може бути одним з таких постачальників ліквідності. В

обмін на свою частку в пулі ліквідності трейдери платять комісію у пул, яка потім розподіляється між постачальниками ліквідності відповідно до їх частки в пулі.

Постачальники ліквідності створюють новий доступний торговий ринок, внісши два токени рівної вартості. Це можуть бути ETH і будь-який токен ERC-20 або два токени ERC-20. Часто ці пули складаються з стейблкоінів, таких як DAI, але це не є обов'язковим. За створення ринків та надання ліквідності для трейдерів постачальники ліквідності Uniswap отримують "токени ліквідності які зазвичай відображають їх частку в усьому пулі ліквідності.

Давайте розкриємо концепцію пулів ліквідності Uniswap на прикладі пулу ліквідності ETH/DAI. У нашій формулі частка ETH в пулу буде позначена як "u а частка DAI - як "t". Що робить Uniswap, так це бере ці дві суми та множить їх, щоб розрахувати загальну ліквідність в пулу - в формулі це буде "N". Основна концепція, що лежить в основі Uniswap, полягає в тому, що "N"завжди повинно залишатися стабільним, що означає, що загальна ліквідність в пулу є постійною.

Отже, формула для загальної ліквідності в пулу:

u * t = N

Наприклад, Девід хоче купити 1 ETH за 1600 DAI, використовуючи пул ліквідності ETH/DAI. Зробивши цю угоду, Девід збільшує кількість DAI в пулі та зменшує кількість ETH. Практично це означає, що ціна ETH зростає, оскільки після транзакції в пулі залишається менше ETH, а ми знаємо, що загальна ліквідність (N) повинна залишатися постійною. Цей механізм визначає формування цін валют у пулі.

1.8 Застосування в різних сферах технологія блокчейн

– **Фінанси і банківська справа:**

Блокчейн використовується для створення безпечних і прозорих систем платежів, поліпшення обліку та розрахунків, а також надання доступу до

фінансових послуг в місцях, де вони раніше були недоступні.

– **Авторські права**

Блокчейн може використовуватися для захисту авторських прав, управління ліцензіями та децентралізованого розподілу контенту, дозволяючи авторам контролювати та отримувати винагороду за свої творчі роботи. Існує багато допоміжних сервісів у цій галузі,такі як: Ascribe, Bitproof, Blockai, Stampery, Verisart, Monegraph, Crypto-Copyrightcrypto-copyright.com, Proof of Existence. Для прикладу Ascribe за допомогою технології блокчейн допомагає зокрема художникам й усім бажаючим підтверджувати й зберігати право на авторство. Ринок Ascribe за допомогою унікальних ідентифікаторів та цифрових сертифікатів для підтвердження авторства й аутентичності дозволяє створювати цифрові видання . Також, в функціонал передбачає механізм передачі права володіння від художника або автора до покупця або колекціонера, включаючи його юридичні аспекти.

– **Енергетика**

Блокчейн може бути застосований для створення децентралізованих систем енергопостачання, обліку та торгівлі енергією, а також для підвищення ефективності енергетичних мереж.

Grid Singularity - децентралізована платформа обміну інформацією в галузі, яка надає ряд додатків для спрощення аналізу даних і тестування, керування інтелектуальними енергетичними системами, роботи з "зеленими сертифікатами"та іншими функціями.

Проект TransActive Grid від LO3 Energy є криптографічно захищеною децентралізованою платформою з відкритим вихідним кодом для застосунків. Вбудовані інструменти бізнес-логіки дозволяють в реальному часі вимірювати рівень виробництва та споживання електроенергії, а також деякі інші показники. Проект знаходиться у стадії розробки, і перша демонстраційна установка в даний час працює у бруклінському районі Нью-Йорка.

– **Електронного голосування**

Використавши безпечність зберігання данних у технології блокчейн можна створити платформу для голосувань.

Follow My Vote розробляє безпечну та прозору платформу для анонімних онлайн-голосувань, що використовує технологію блокчейн та еліптичну криптографію для забезпечення точності та достовірності результатів. Вихідний код проекту є відкритим.

– **Відеоігри**

Блокчейн може використовуватись у відеоіграх для зберігання і обробки інформації.

Etheria - віртуальний світ, де гравці намагаються заволодіти клітинками грального поля, добуваючи їх за допомогою блоків та будуючи на них щось. Усі дані, що описують світ та його стан, а також усі дії гравців, зберігаються в децентралізованому блокчейні Ethereum.

First Blood - платформа, яка дозволяє кіберспортсменам кидати одне одному виклик у різних ігрових дисциплінах, фанатам - ставити або судити ігри, а також організовувати турніри та отримувати винагороду за будь-яку подібну діяльність. First Blood працює на базі блокчейна Ethereum з власним токеном 1ST і активно використовує смарт-контракти для обробки результатів та оракулів як джерела інформації про результати матчів.

– **Керування данними**

Factom - визначна блокчейн-компанія, яка застосовує розподілені реєстри поза фінансовою сферою, зокрема, у сфері керування даними. Ідентифікаційні блокчейни компанії використовуються для реалізації систем керування базами даних та аналізу даних у різних галузях. Бізнеси, уряди, неприбуткові організації користуються Factom для спрощення процедур ведення записів та фіксації інформації про бізнес-процеси. Factom дозволяють клієнтам здійснювати свою діяльність відповідно до вимог безпеки та нормативно-правового регулювання їх ринку. Усі записи в Factom мають відмітки часу та зберігаються в блокчейнах, що дозволяє знизити витрати і складність їх управління,

аудиту та відповідності вимогам регуляторного законодавства.

–

1.9 Майнінг машини

Майнінг машини є спеціальними пристроями, розробленими для видобутку криптовалют, зокрема Bitcoin і інших криптовалют, що використовують алгоритм Proof-of-Work. Ці машини спроектовані для вирішення складних математичних завдань, які підтверджують транзакції в мережі і додають нові блоки до блокчейну.

Щоб успішно додати блок, майнери Bitcoin змагаються у вирішенні надзвичайно складних математичних задач, для яких потрібні дороговартісні комп'ютери і величезні кількості електроенергії. Щоб завершити процес майнингу, майнери мають бути першими, хто знаходить правильну або найближчу відповідь на поставленого питання. Процес вгадування правильного числа (хешу) відомий як proof of work. Гірники вгадують цільовий хеш, роблячи випадкові спроби якомога швидше, що вимагає значних обчислювальних потужностей. Складність лише збільшується з приєднанням нових майнерів до мережі.

Комп'ютерне обладнання, необхідне для цього процесу, відоме як спеціалізовані інтегральні схеми (ASIC), і може коштувати до 10 000 доларів. ASIC витрачають величезні кількості електроенергії, що викликало критику з боку екологічних груп та обмежує прибутковість майнерів.

Якщо майнеру вдається успішно додати блок до блокчейну, він отримує винагороду у розмірі 6,25 біткоїнів. Сума винагороди зменшується приблизно наполовину кожні чотири роки, або кожні 210 000 блоків. На березень 2023 року Bitcoin торгувався приблизно за 24 300 долари, що робить 6,25 біткоїнів вартістю 152 000 доларів.

Чи вигідний майнінг біткойнів залежить від випадку. Навіть якщо біткойн-майнери досягнуть успіху, незрозуміло, що їхні зусилля принесуть

прибуток через високі початкові витрати на обладнання та поточні витрати на електроенергію. Відповідно до звіту Дослідницької служби Конгресу за 2019 рік, електроенергія для одного ASIC може використовувати стільки ж електроенергії, скільки півмільйона пристроїв PlayStation 3 .

З огляду на зростання складності та витрат на майнінг біткойнів, майнерам потрібна все більша обчислювальна потужність. За даними Cambridge Bitcoin Electricity Consumption Index, річне споживання електроенергії на майнінг біткойнів становить приблизно 121 терават-годину, що перевищує енергоспоживання більшості країн. На серпень 2021 року, для видобуття одного біткойна знадобиться електроенергія, еквівалентна витратам типового американського домогосподарства протягом 9 років.

Один із способів зниження витрат на майнінг - приєднання до майнінгового пулу. Пули дозволяють майнерам об'єднувати свої ресурси та отримувати більше можливостей, але розділені винагороди означають менші індивідуальні виплати. Нестабільність ціни біткойна також ускладнює точне визначення суми, за яку працюють майнери.

Необхідні атребути для майнінгу :

Гаманець. Усі біткоїни, які ви заробите внаслідок своїх зусиль у галузі майнінгу, будуть зберігатися тут. Гаманець - це зашифрований онлайн-обліковий запис, який дозволяє зберігати, передавати та отримувати біткоїни або інші криптовалюти. Компанії, такі як Coinbase, Trezor та Exodus, пропонують варіанти гаманців для криптовалюти.

Програмне забезпечення для майнінгу. Існує кілька постачальників програмного забезпечення для майнінгу, багато з яких можна завантажити безкоштовно, і вони працюють на комп'ютерах з Windows та Mac. Як тільки програмне забезпечення буде підключено до необхідного обладнання, ви зможете добувати біткоїни.

Комп'ютерне обладнання. Найвитратнішим аспектом майнінгу біткоїнів є апаратне забезпечення. Вам знадобиться потужний комп'ютер, який споживає велику кількість електроенергії, щоб успішно добувати

біткоїни. Вартість апаратного забезпечення часто становить близько 10 000 доларів або більше.

Висновки до розділу 1

В сучасному інформаційному суспільстві блокчейн технологія стала одним із самих актуальних і перспективних напрямків розвитку. У першій частині цієї роботи розглядаємо основи блокчейн технології, починаючи з її створення та понятійного апарату. Зокрема, вивчимо процес становлення блокчейн і визначимл сутність цієї технології. Далі, проведемо аналіз переваг блокчейн і вилучимо основні поняття протоколу блокчейн. Розглянемо різні протоколи блокчейн, включаючи Automated Market Maker і Uniswap, а також вивчимо їх функціональність і застосування. Нозглядаємо різні сфери застосування технології блокчейн. Також розбираэмо поняття майнінг машини.

2 ПРОТОКОЛ CONSTANT PRODUCT

У сучасному фінансовому світі децентралізована фінансова система (DeFi) займає дедалі більшу роль. У другій частині цієї роботи ми заглибимося у дослідження протоколу Constant Product, який є одним із ключових елементів DeFi. Для початку визначимо сутність децентралізованої фінансової системи та розглянемо роль децентралізованих бірж (DEX) у цій системі. Потім ми вивчимо децентралізоване криптовалютне кредитування та його взаємозв'язок із протоколом Constant Product.

Протокол Constant Product є основою створення концепції Constant Product Market, який дозволяє обмінювати різні криптовалюти з використанням стійких коефіцієнтів. Ми детально розглянемо основи Constant Product Market та проаналізуємо процес обміну та умови ліквідації в рамках цього протоколу.

2.1 Що таке децентралізована фінансова система (DeFi)?

Децентралізована фінансова система (DeFi) - це нова модель організації та забезпечення транзакцій, обмінів і фінансових послуг на основі криптовалюти.

Основна ідея DeFi полягає в тому, що відсутня централізована влада, яка б диктувала або контролювала операції. Це відрізняється від традиційних моделей фінансових систем для фіатних валют або централізованих фінансових систем (CeFi) на ринках криптовалюти. У централізованих моделях існує основна влада, яка може впливати і контролювати потік транзакцій. Часто центральна влада також відповідає за зберігання активів.

У випадку DeFi відсутня центральна влада. Замість цього влада

розподіляється у децентралізованому підході, який призначений надати більше сили та контролю індивідуумам. У моделі DeFi всі транзакції з покупки, продажу, кредитів і платежів з використанням криптовалюти можуть відбуватись без центральної влади в підході «рівний до рівного» (peer-to-peer, P2P).

Зберігання активів є фундаментальною складовою будь-якої фінансової моделі. У підході DeFi окремі трейдери мають контроль над своїми приватними криптографічними ключами, які забезпечують зберігання криптовалютних активів. Фінансові транзакції в моделі DeFi здійснюються за допомогою смарт-контрактів, які часто підтримуються на блокчейнах, заснованих на Ethereum.

Модель DeFi також включє поняття децентралізованих обмінників (DEX), які діють з метою з'єднання та забезпечення можливості виконання транзакцій з криптовалютою між індивідуальними користувачами. DeFi також часто пов'язується з концепцією децентралізованих додатків (dApps), зазвичай використовуваних у фінансових послугах.

2.2 Децентралізовані біржі (DEX)

Це важна складова децентралізованого фінансового ринку. DEX-біржі дозволяють торгувати криптовалютами без необхідності довіряти свої кошти централізованим організаціям.

Такі платформи працюють на блокчейні і дають трейдерам змогу здійснювати угоди безпосередньо між рахунками. Для початку торгівлі не потрібно реєстрації та верифікації, достатньо просто синхронізувати гаманець зі смарт-контрактом. Іншими словами, користувачі можуть зберігати свою анонімність.

Проте у децентралізованих бірж є й недоліки. Один з основних - низька ліквідність порівняно з централізованими платформами. Це може спричинити певні труднощі для трейдерів:

Неможливість придбати необхідну кількість токенів через недостатню кількість продавців на біржі.

Неможливість продати активи через недостатню кількість покупців.

Такі проблеми частково вирішуються завдяки агрегаторам, які збирають ліквідність з кількох бірж. Проте навіть вони не завжди дозволяють здійснити угоду на значну суму.

Однак з розвитком ринку децентралізованих бірж поступово поліпшується їх функціональність. Їх популярність зростає, і вони стають важливим елементом у майбутньому фінансової індустрії.

2.3 Децентралізоване криптовалютне кредитування

Існують DeFi-сервіси, які надають можливість брати кредити. Зазвичай для цього потрібно надати криптовалюту як заставу, а у позику можна взяти стейблкоіни.

Такий вид кредитування має кілька переваг порівняно з аналогічними послугами традиційних банків:

– Не потрібно надавати документи.

– Гроші надходять миттєво.

– Кредит можна брати на будь-який строк.

– Відсоткові ставки значно нижчі.

– Заборгованість можна погашати частинами та з будь-якою періодичністю.

Щоб взяти кредит, потрібно виконати такі дії:

1) Синхронізувати свій гаманець зі спеціальним смарт-контрактом.

2) Вказати бажані умови - суму, заставний актив і т.д.

3) Підтвердити угоду в блокчейні.

Після цього з рахунку позичальника будуть списані монети, які надаються як забезпечення, і на їх місце прийдуть стейблкоіни. У більшості випадків вартість застави перевищує суму кредиту на 10-50

Розберемо чому взігалі брати кредит , якщо можна просто продати

криптовалюту і отримати гроші. Справа в тому, що трейдери та інвестори активно використовують подібні сервіси для хеджування ризиків.

Уявімо таку ситуацію:

– У інвестора є 10 ETH.

– За поточним курсом 1 ETH коштує 2000 доларів.

Отже, загальна сума активів становить 20 000 доларів. Користувач вважає, що в майбутньому ефір зросте в ціні. Але зараз йому потрібні гроші для якихось цілей, наприклад, для торгівлі на ринку. Тоді він може взяти кредит під заставу своїх ETH.

Якщо згідно з умовами платформи вартість застави має перевищувати суму кредиту на 50 відсотків, інвестор отримає в позику 10 000 USDT на свої 10 ETH. Далі ситуація може розвиватися наступним чином:

Якщо курс ETH зросте, наприклад, до 3000 доларів, інвестор зможе сплатити 10 000 USDT, щоб отримати назад свої ефіри, які вже коштують 30 000 доларів.

Якщо курс впаде нижче 1000 доларів, позиція буде автоматично ліквідована. В результаті кредитор отримає 10 ETH, а позичальник залишиться зі своїми 10 000 USDT. Поріг ліквідації залежить від умов конкретного сервісу.

Таким чином, якщо курс монети зросте, позичальник отримає всю прибуток, а якщо впаде, він частково зафіксує свою позицію. При цьому отриманими в кредит грошима можна розпоряджатися на свій розсуд.

Комісії за користування кредитом для стейблкоінів рідко перевищує декілька відсотків річних. Кредитори, зі свого боку, можуть використовувати аналог банківського депозиту з підвищеними інвестиційними відсотками. В результаті обидва отримують вигідні умови завдяки відсутності посередника.

2.4 Constant Product Market

Умовні позначення

– Великі латиньскі літери (U, T, L) - тип активу.

– Маленькі латиньскі літери (u, t, l) - відповідно вартість активу, кількість одиниць.

– $\Delta_1 u$,$\Delta_2 u$ - деякі сумми активу U такі, що $\Delta_1 u + \Delta_2 u = \Delta u$.

– $\Delta_1 t$,$\Delta_2 t$ - вудповідні необхідні сумми для торгівлі $\Delta_1 u$,$\Delta_2 u$.

– Δt вартість активу T, що отримаємо за торгівлю Δu активу U.

– Функція $F_{U/T}(h; u)$ - кількість активу T, що можна отримати в момент h, продавши u активу U.

– φ - комісієя за транзакцію у відсотках або $\kappa = 1 - \varphi$.

–

2.4.1 Constant Product Market

Constant Product Market базуеться на формулі, яка залишається незмінною незалежно від розміру угоди чи активу, яким торгує. Правила для такої угоди і зміни цін, які її супроводжують, завжди однакові.

Більшість AMM використовують моделі Constant Product Market. Формула для цієї моделі: u * t = N. У цій формулі загальний обсяг ліквідності повинен залишатися постійним. У наших позначеннях літера N. u та t представляють дві токени, які інвестуються в пул ліквідності. Значення цих двох токенів завжди повинно дорівнювати N. Тому, збільшуючи значення u, значення t має зменшуватися і навпаки.

Припустимо Constant Product Market(постійний товарний ринок) складається з двох активів: U,T, з відповідними вартостями u і t.Вартість u одиниць активу U рівна вартості t одиниць активу .

Запишемо константу $N = u * t$.

Введемо значення φ - комісієя за транзакцію у відсотках або $\kappa = 1 - \varphi$

Трейдер хоче купити Δt активу . Тоді вартість Δu активу U розраховується з рівняння: $(t - \Delta t)(u + \kappa\Delta u) = N$,

$\Delta u = \frac{u*\Delta t}{\kappa(t-\Delta t)}$

Після обміну отримуємо новий стан ринку $N^{'} > N$.

$N^{'} = (t-\Delta t)(u+\Delta u) = N-\Delta t*u+(t-\Delta t)\Delta u = N+\Delta t*u(\frac{1}{\kappa}-1) > N$

Звернемо увагу, що якщо припустити нульову комісію, відповідно множник $(\frac{1}{\kappa} - 1)$ нульвий, то добуток залишится сталим, незважаючи на будь-яку кількість угод, звідси і назва"Constant Product".

2.4.2 Аніліз процесу обміну

Розглянемо два випадки:

– обмін усієї кількості активу Δu на Δt

– обмін деякої частини Δu $(\Delta_1 u)$ на $\Delta_1 t$, а потім другої частини $(\Delta_2 u)$ на $\Delta_2 t$

Розглянемо і виведемо як співвідноситься отриманий актив Δt з першого випадку обміну до суми $\Delta_1 t + \Delta_2$ з другого випадку обміну.

Обмежимо вартість $\Delta_1 t + \Delta_2 t$ знизу

Для першого випадку з формули моделі Constant Product Market

$N = t * u = (t - \Delta t)(u + \kappa\Delta u)$

виразмо цікавлячу нас вартість Δt:

$\Delta t = t - \frac{ut}{u+\kappa\Delta u} = t - \frac{N}{u+\kappa\Delta u} = \frac{\kappa\Delta u*t}{u+\kappa\Delta u}$

Для другого випадку обміну після першого свапу вартість отриманого активу:

$\Delta_1 t = t - \frac{N}{u+\kappa\Delta_1 u}$

Запишемо новий стан системи:

$N^{'} = u^{'} * t^{'} = (u + \Delta_1 u)(t - \Delta_1 t)$

Для другого випадку обміну після другого свапу вартість отриманого активу:

$\Delta_2 t = t^{'} - \frac{N^{'}}{u^{'}+\kappa\Delta_2 u}$

Отже для другого випадку обміну, після обох свапів ми отримаємо:

$\Delta_1 t + \Delta_2 t = t - \frac{N}{u+\kappa\Delta_1 u} + t' - \frac{N'}{u'+\kappa\Delta_2 u}$

Виразимо і змінюємо t' з рівняння новогу стану системи:

$\Delta_1 t + \Delta_2 t = t - \frac{N}{u+\kappa\Delta_1 u} + t' - \frac{N'}{u'+\kappa\Delta_2 u} \pm \frac{N}{u+\kappa\Delta u} =$

$= (t - \frac{N}{u+\kappa\Delta u}) + \frac{N}{u+\kappa\Delta u} - \frac{N}{u+\kappa\Delta_1 u} + \frac{N'}{u+\Delta_1 u} - \frac{N'}{u'+\kappa\Delta_2 u}$

Зауважимо, що $u' + \kappa\Delta_2 u = u + \Delta_1 u + \kappa\Delta_2 u$:

$\Delta_1 t + \Delta_2 t = \Delta t + N(\frac{1}{u+\kappa\Delta u} - \frac{1}{u+\kappa\Delta_1 u}) + N'(\frac{1}{u+\Delta_1 u} - \frac{1}{u'+\kappa\Delta_2 u}) =$

$= \Delta t - N * \frac{\kappa\Delta_2 u}{(u+\kappa\Delta u)(u+\kappa\Delta_1 u)} + N' * \frac{\kappa\Delta_2 u}{(u+\Delta_1 u)(u+\Delta_1 u+\kappa\Delta_2 u)} =$

$= \Delta t + \kappa\Delta_2 u(\frac{N'}{(u+\Delta_1 u)(u+\Delta_1 u+\kappa\Delta_2 u)} - \frac{N}{(u+\kappa\Delta u)(u+\kappa\Delta_1 u)}) =$

$= \Delta t + \kappa\Delta_2 u(t - \Delta_1 t)(\frac{1}{u+\Delta_1 u+\kappa\Delta_2 u} - \frac{1}{(u+\kappa(\Delta_1 u+\Delta_2 u))}) =$

$= \Delta t + \frac{(\kappa-1)\kappa*\Delta_1 u*\Delta_2 u(t-\Delta_1 t)}{(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa(\Delta_1 u+\Delta_2 u))}$

Або інакше :

$\Delta t = \Delta_1 t + \Delta_2 t + \frac{(\kappa-1)\kappa*\Delta_1 u*\Delta_2 u(t-\Delta_1 t)}{(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa(\Delta_1 u+\Delta_2 u))}$

Отже, отримуємо співвідношення, що дає змогу оцінити нижню межу

$\Delta t \geqslant \Delta_1 t + \Delta_2 t.$

Обмежимо вартість $\Delta_1 t + \Delta_2 t$ зверху

Для першого випадку з формули моделі Constant Product Market:

$\Delta t = t - \frac{ut}{u+\kappa\Delta u} = \frac{\kappa\Delta u*t}{u+\kappa\Delta u}$

Для другого випадку обміну після першого свапу вартість отриманого активу:

$\Delta_1 t = t - \frac{u*t}{u+\kappa\Delta_1 u} = \frac{\kappa t\Delta_1 u}{u+\kappa\Delta_1 u}$

$t - \Delta_1 t = \frac{u*t}{u+\kappa\Delta_1 u}$

Використовуючи рівність, що ми отримали для нижньої межі:

$\frac{\Delta_1 t+\Delta_2 t}{\Delta t} = 1 - \frac{(1-\kappa)\kappa*\Delta_1 u*\Delta_2 u(t-\Delta_1 t)}{\Delta t(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa(\Delta_1 u+\Delta_2 u))} = 1 - \Delta$

$\Delta = \frac{(1-\kappa)\kappa*\Delta_1 u*\Delta_2 u(t-\Delta_1 t)}{\Delta t(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa(\Delta_1 u+\Delta_2 u))}$

Враховуючи що $1 - \kappa = \varphi > 0$, $\Delta > 0$.

Підставимо $\Delta t = \frac{\kappa\Delta u*t}{u+\kappa\Delta u}$ і $t - \Delta_1 t = \frac{u*t}{u+\kappa\Delta_1 u}$ у Δ.

Отримаємо:

$\Delta = \frac{(1-\kappa)\kappa\Delta_1 u\Delta_2 u*\frac{ut}{u+\kappa\Delta_1 u}}{\frac{\kappa\Delta u*t}{u+\kappa\Delta u}(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa\Delta_1 u+\kappa\Delta_2 u)} = \frac{(1-\kappa)\Delta_1 u\Delta_2 u*u}{\Delta u(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa\Delta u)} =$

$= (1-\kappa) * \frac{\Delta_2 u}{\Delta u} * \frac{\Delta_1 u}{u+\Delta_1 u+\kappa\Delta_2 u} * \frac{u}{u+\kappa\Delta u} \leqslant (1-\kappa)$

Далі зробимо деякі перетворення для комформтного використання:

$\frac{\Delta_1 t+\Delta_2 t}{\Delta t} = 1 - \frac{(1-\kappa)\kappa * \Delta_1 u * \Delta_2 u(t-\Delta_1 t)}{\Delta t(u+\Delta_1 u+\kappa\Delta_2 u)(u+\kappa(\Delta_1 u+\Delta_2 u))} = 1 - \Delta$:

$\frac{\Delta_1 t+\Delta_2 t}{\Delta t} \geqslant 1 - (1-\kappa) = \kappa$

Або інакше : $\Delta_1 t + \Delta_2 t \geqslant \kappa * \Delta t$

Обьеднавши виведені обмеження отримаємо нерівність:

$\kappa * \Delta t \leqslant \Delta_1 t + \Delta_2 t \leqslant \Delta t.$

Враховуючи, що κ близька до 1, функцію $F_{U/T}(h; u)$ близька до лінійної.

Оцінимо збитки від повторних обмінів.

Нехай в пули спочатку було Δu одиниць активу U та Δt одиниць активу T. Далі було зроблено дві транзакції:

– Помістили Δu одиниць активу U у пул і забрали відповідну кількість Δt одиниць активу T.

– Відразу помістили Δt одиниць активу T у пул і забрали відповідну кількість $\Delta_1 u$ одиниць активу U.

$N = u * t$

Після першого свапу:

$\Delta t = \frac{\kappa\Delta u * t}{u+\kappa\Delta u}$

$u' = u + \Delta u$, $t' = t - \Delta t$

Новий стан системи:

$N' = u' * t' = (u + \Delta u)(t - \Delta t)$

$(u' - \Delta_1 u)(t' + \kappa\Delta t) = u' * t' = N'$

$\Delta_1 u = u' - \frac{N'}{t'+\kappa\Delta t} = u'(1 - \frac{t'}{t'+\kappa\Delta t}) = \frac{\kappa u'\Delta t}{t'+\kappa\Delta t}$

Підставимо $\Delta t = \frac{\kappa\Delta u * t}{u+\kappa\Delta u}$:

$\Delta_1 u = \frac{\kappa u'\kappa t\Delta u}{(t'+\kappa\Delta t)(u+\kappa\Delta u)} = \frac{\kappa^2 t\Delta u(u+\Delta u)}{(t-\Delta t+\kappa\Delta t)(u+\kappa\Delta u)} = \frac{\kappa^2 t\Delta u(u+\Delta u)}{(t-\Delta t(1-\kappa))(u+\kappa\Delta u)}$

$\Delta_1 u = \kappa^2 t\Delta u * \frac{t}{(t-\Delta t*\varphi)} * \frac{(u+\Delta u)}{(u+\kappa\Delta u)} \geqslant \kappa^2 * \Delta u$

Отже: $\kappa^2 * u \leqslant \Delta_1 u \leqslant u$

2.4.3 Умови ліквідації

Розглянемо три різні активи U, T, L. Відкриваючи торгову позицію з кредитним плечем, Трейдер використовує наявний у нього актив L-депозит у розмірі l_0 одиниць, позичає актив U у розмірі u одиниць і обмінює їх на t одиниць активу T .

$u \leqslant s_{max} * F_{L/U}(h_0; l_0)$ -прийнятна сума позикового активу в u одиниць.

$S_{max} = s_{max} + 1$ -максимально прийняте кредитне плече.

$l = F_{L/U}(h_0; l_0)$

$S = \frac{l+u}{l}$

При закритті транзакції ліквідацією в якийсь момент h відбувається зворотна транзакція, яка обмінює t одиниць активу T на $u(h)$ одиниць активу U: $u(h) = F_{T/U}(h; t)$.

Нехай позиція була відкрита в момент $h_0 = 0$ і вимушена закритисьв момент $h_0 \geqslant 0$. Припускаємо, що процес закриття позиції вимагає деякого часу, через затримку на виконання транзакції у блокчейн, обмежемо цей час десятью хвилинами. Будемо вважати, що під час виконання транзакції максимальна частка падіння активу T відносно активу U не перевищує певного значення $\lambda \in (0,1)$. Після завершення транзакції отримуємо не менше $(1 - \lambda) * u(h)$ одиниць активу U. З цієї суми необхідно погасити борг u_0 одиниць активу U,яку трейдер позичив під заставу ,комісію трейдера за позику, нарахована за поточною річною ставкою позики (BAR) за формулою складних відсотків і частину комісії за позику трейдера, яка нараховується в період ліквідації.

Комісія трейдера за позику протягом інтервалу часу h розраховується за секунду на основі поточної річної ставки, як складений відсоток позикової ліквідності. Припустимо кількість секунд у період h -R_h, що поділена на z періодів стабільності річної ставки позики $R_h = r_1 + ... + r_z$ (r_i- кількість секунд в i-тому пероді стабільності). η_i –

значення поточної річної ставки позики за період, поділене на кількість секунд на рік (31536000).

Отже, повну вартість платежів трейдера за використання u_0 одиниць активу U протягом часу h: $\chi(h) = (1+\eta_1)^{r_1} * ... * (1+\eta_z)^{r_z}$

З обраними допущеннями, період ліквідації обмежений 600 секундами, а максимальне значення поточної річної ставки позики становить 1000 відсотків . Таким чином, навіть якщо значення поточної річної ставки позики різко зросте до максимуму протягом періоду ліквідації, загальний комісія трейдера за позику з моменту відкриття позиції до моменту її закриття буде не більше, ніж:

$\Delta * \chi(h)u_0 = (1 + \frac{10}{31536000})^{600} * \chi(h)u_0$

Де $\Delta = 1 + 2 * 10^{-4} = 1.0002$

Отже, щоб усі платежі були сплачені необхідно виконання умови: $(1-\lambda) * u(h) \geqslant \Delta * \chi(h)u_0$.

З цього випливає, що умова ліквідації $(1-\lambda) * u(h) \leqslant \Delta * \chi(h)u_0$.

$u'(h) = (1-\lambda) * u(h) - \Delta * \chi(h)u_0$-кількості одиниць активу U, яка залишається після здійснення всіх платежів, з урахуванням можливого падіння вартості активу T та максимальне значення поточної річної ставки позики під час закриття позиції.

Відповідно до умови ліквідація повинна розпочатися негайно після його відкриття, якщо виконується наступна умова:

$(1-\lambda) * u(0) \leqslant \Delta * \chi(0)u_0 = \Delta u_0$

Щоб уникнути такої ситуації , оберемо S_{max} при якому буде виконуватися нерівність :

$(1-\lambda) * u(0) > \Delta u_0$

Використаємо виведені властивості:

$u(0) = F_{T/U}(0;t) = F_{T/U}(0; F_{U/T}(0;u_0) + F_{L/T}(0;l_0)) \geqslant F_{T/U}(0; F_{U/T}(0;u_0)) + F$

$u(0) \geqslant \kappa^2 * u_0 + F_{T/U}(0; F_{L/T}(0;l_0))$

Оскільки $u(0) = (S-1)* = F_{L/U}(0;l_0)$ можемо записати нерівність, за умову, що ліквідація позиції не починається в момент її відкриття:

$(1-\lambda)(\kappa^2 * (S-1) * F_{L/U}(0;l_0) + F_{T/U}(0; F_{L/T}(0;l_0)) > \Delta * (S-1) * F_{L/U}(0;l_0)$

$F_{T/U}(0; F_{L/T}(0; l_0)) \geqslant F_{T/U}(0; F_{U/T}(0; l_0)) \geqslant \kappa^2 * F_{T/U}(0; t)$

Отже для виконання нерівності $(1-\lambda)(\kappa^2*(S-1)*F_{L/U}(0; l_0)+F_{T/U}(0; F_{L/T}(0; l_0)) > \Delta*(S-1)*F_{L/U}(0; l_0)$ достатньо виконати:

$(1 - \lambda)(\kappa^2(S - 1)F_{L/U}(0; l_0) + \kappa^2 F_{L/U}(0; l_0) > \Delta(S - 1)F_{L/U}(0; l_0)$

Або: $(1 - \lambda) * \kappa^2 * S > \Delta(S - 1)$

Отже, отримуємо обмеження на максимальне значення кредитного плеча:

$S_{max} < \frac{\Delta}{\Delta - \kappa^2(1-\lambda)}$

Обчислимо максимальне значення кредитного плеча для пари BUSD/USDT

Після проведення дослідження на інвестаційному ресурсу binance.com пар BUSD/USDT та USDT/BUSD, з'ясовано, що волотильність даної пари за останні 3 роки не перевищувала 7 відсотків.

Розглянемо найгірший випадок $\lambda = 0.07$.

Враховуючи $\kappa^2 * u \leqslant \Delta_1 u$, $\kappa = 0.2$.

$S_{max} < \frac{1.0002}{1.0002 - 0.2*(1-0.07)}$

$S_{max} < 1.228$

Отже, макимальне кредитне плече для пари BUSD/USDT = 1.

Висновки до розділу 2

В другому розділі оглянуто поняття децинтралізована фінансова система (DeFi), децентралізовані біржі (DEX) та процесс криптовалютного кредитування. Зокрема досліджено DeFi протокол на базі Constant Product Market. Розглянуто два випадкі обмінів і виведено співвідношення вартостей обмінів між собою. Виведено умову ліквідації та обчислено максимальне кредитне плече. Це дослідження допоможе трейдорам та кріпто-інвесторам безпечно та прибутково керувати своїми активами.

ВИСНОВКИ

у ході даної роботи ми дослідили блокчейн-технологію та основні концепції, пов'язані з нею, такі як Hyperledger, Multichain та Enterprise Ethereum. Кожен з цих протоколів має свої унікальні особливості та застосування у бізнес-середовищі. Загалом, використання блокчейну має широкі можливості, а його значимість зростає з кожною хвилиною, оскільки вже продемонстрував свою цінність у різних галузях та має потенціал для подальшого розвитку та інновацій. Розглянули децентралізовану фінансову систему DeFi та децентралізовані біржі DEX.

Аналізували два випадки обміну активами на Constant Product Market, що складається з активів U і T. У першому випадку, коли обмінюється вся кількість активу U на актив T, було отримано формулу для розрахунку вартості активу T після обміну, яка враховує комісію за транзакцію та дозволяє знаходити новий стан ринку. У другому випадку розглядалася ситуація, коли обмін відбувається частинами. За допомогою формул було встановлено нерівність, яка дозволяє оцінити нижню межу значення активу T після обміну, а також формулу для розрахунку верхньої межі значення активу T. Обидві формули враховують комісію за транзакцію і дозволяють оцінити межі зміни значень активів після обміну.

Також розглядається процес відкриття торгової позиції з кредитним плечем, де трейдер використовує активи L-депозиту, позичає актив U та обмінює їх на актив T. При закритті позиції вимагається час транзакції та певна частка падіння активу T відносно активу U. Комісія трейдера за позику розраховується на основі поточної річної ставки позики та кількості секунд у періоді. Запропоновано умову початку ліквідації позиції негайно після її відкриття, що означає, що в разі незадовільного руху активів трейдер має змогу негайно ліквідувати позицію для запобігання подальших втрат. Для забезпечення цього був обраний

параметр S_{max} , який гарантує, що умова ліквідації буде виконуватися.

Результати роботи представлені у вигляді формул та розрахунків, що демонструють математичний підхід до оцінки та управління ризиками в торговельних операціях з використанням кредитного плеча. Ці дані можуть бути використані трейдерами для зрозуміння потенційних ризиків і прийняття обґрунтованих рішень щодо управління своїми позиціями.

ПЕРЕЛІК ПОСИЛАНЬ

1. URL: https://www.binance.com/uk-UA

2. Daniel Drescher (2017) Blockchain Basics: A Non-Technical Introduction in 25 Steps

3. Antonopoulos, A. M. (2020). Mastering Ethereum: Building Smart Contracts and DApps.

4. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

5. Sikorka, P., Teutsch, J., Bocek, T. (2020). A Brief History of Uniswap and Automated Market Makers.

6. Guillermo Angeris, Tarun Chitra (2020) Improved Price Oracles: Constant Function Market Makers

7. Darren Lau, Daryl Lau, Te Se Jin, Christian Kho, Erina Azmi, T.M. Lee, Bobby Ong (2020) How is DeFi

8. Liu, Y., Livshits, B. (2021). A Survey on Decentralized Finance (DeFi).

9. ConsenSys. (2020). DeFi: Building the Future of Finance.

10. Martínez, S. (2021). The Decentralized Exchange Revolution: Unleashing the Power of Blockchain and Smart Contracts.