|  |  |  |  |
| --- | --- | --- | --- |
| МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Тараса Шевченка ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ  **Кафедра програмних систем і технологій**  Дисципліна  **«**МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ**»**  **Лабораторна робота № 3**  «Імітаційні моделі» | | | |
| **Виконав:** | Гоша Давід | **Перевірив**: |  |
| Група | ІПЗ-33 | Дата перевірки |  |
| Форма навчання | денна | Оцінка |  |
| Спеціальність | 121 |
| 2022 | | | |

**Тема (завдання) для дослідження** – Імітаційна модель систем на основі Blockchain технології з використанням теорії масового обслуговування.

**Аналіз предметної області** – У 2008 році анонімна особа або група під псевдонімом «Сатоші Накамото» представила автоматизовану систему безготівкових платежів і назвала її «біткойн» (цифрова валюта). Ця система цифрової валюти P2P мала на меті запобігти участі третіх сторін у фінансових транзакціях у анонімному та захищеному(надійному) протоколі. У січні 2009 року та сама група чи особа розробила програмне забезпечення у вигляді відкритого коду та запустила першу цифрову валюту в історію. Базовою технологією біткойна є блокчейн, який забезпечує послідовний і незмінний упорядкований список блоків транзакцій, з’єднаних разом, при цьому всі однорангові мережі P2P підтримують свою власну копію блокчейну, відому як леджер.

Основним протоколом валюти біткойн є консенсус, який вимагає, щоб усі однорангові мережі погоджувалися щодо кожного окремого запису блоку в розподіленому блокчейні. Останнім часом блокчейни привернули величезну увагу кількох дослідників. Поява технології блокчейн у формі цифрових валют вплинула на багато інших сфер, таких як електронна охорона здоров’я, електронні фінанси, нерухомість, електронне голосування, ланцюги поставок, розумні будинки, розумні міста, Інтернет речей, і так далі. Популярність блокчейнів є природною, оскільки вони можуть надавати бажані функції, замінюючи архітектури централізованої взаємодії. Але проблема з біткойнами полягає в тому, що для забезпечення безпеки та цілісності системи потрібні трудомісткі процеси; і майнінг біткойнів вважається процедурою, що потребує багато часу та ресурсів.

Було кілька спроб скоротити необхідний час і підвищити продуктивність шляхом зміни характеристик базових алгоритмів. Нові криптовалюти, схожі на біткойн, називаються альтернативними монетами; на даний момент Ethereum, Binancecoin, Dash, DogeCoin, LiteCoin, Solana і Ripple є найвідомішими валютами, на створення яких надихнув біткойн. На сьогодні існує 2116 криптовалют, і більшість з них створено на тій же розподіленій технології блокчейну, хоча й із зміненим набором принципів і покращеними характеристиками.

Оскільки більшість додатків реалізують блокчейн, аналітичне моделювання та імітація систем блокчейну є важливими для оцінки продуктивності та спостережень за поведінкою. На жаль, менше зусиль було присвячено імітаційному моделюванню блокчейнів; Статей в літературі дуже мало, і майже всі вони лише аналітичне моделювання біткойна. Quan-Lin Li описав весь блокчейн, зокрема лише операції майнінгу, використовуючи одну чергу; транзакції в черзі передбачалися для процесу створення блоку, а транзакції в обслуговуванні передбачалися для процесу створення блоку. Yoshiaki Kawase надав дослідження теорії черги, щоб представити час підтвердження транзакцій для Bitcoin. Деякі роботи також були описаны з точки зору теорії ігор.

**Мета практикуму** – Розробка моделі, заснованої на теорії масового обслуговування, для розуміння робочих і теоретичних аспектів блокчейна.

**Гіпотеза** –

**Математичний опис моделі**

Як зображено на рисунку [3](#_bookmark4), ми розділили мережу блокчейн на два типи пулів:

* Перший тип вузлів має справу з непідтвердженими транзакціями в Memory-pool, де транзакції, згенеровані різними користувачами, накопичуються для відправки майнерам.
* Другий - мережа вузлів Майнінг (Mining-pool);

Ці бенкети мереж вибирають транзакції з пулу пам'яті, щоб згенерувати блок і почати їх видобуток. У будь-який момент часу в майнінг-пулі може бути тільки один блок. Однак всередині майнінг-пулу майнінг-завдання можна розділити на численні множинні завдання або потоки для паралельної обробки в декількох вузлах видобутку в мережі. Але всі ці робочі місця повинні бути частиною одного блоку, як тільки робота з видобутку блоку буде виконана, всі частини знову об'єднуються на станції приєднання і відправляються до решти мережі.

**Розрахунок параметрів моделювання**

На момент написання роботи в біткойні середня кількість транзакцій на блок - 2002, середня кількість підтверджених транзакцій в секунду – 3.056, а середня кількість блоків в день – 144. Однак середній розмір транзакції можна розрахувати за розміром блокчейну/загальною кількістю транзакцій, яка зросла з 308 тo 560 байт з 2011 по 2022 рік. Крім того, зберігаючи обмеження Біткойна, що розглядаються, як жорстко закодовані в блокчейні для Біткойн:

* Розмір блоку не повинен перевищувати 1 Мегабайт
* Час генерації блоку та майнінгу має становити 600 секунд (10 хвилин)

Для моделі оберем найбільші показники. Розглянемо, що одна транзакція розміром 500 байт і 1 Мегабайт дорівнює 1.048.576 байтам; таким чином, 1.048.576 ÷ 500 ≈ 2100 транзакцій на блок, тому 2100 ÷ 600 = 3,5 – це середня кількість підтверджених транзакцій в секунду, а всього видобуто 144 блоки, при цьому 2100 × 144 = 302.400 - загальна кількість транзакцій за день. Кількість блоків, βn, можна розрахувати за допомогою:

де T – загальний час , а βt - час майнінгу блока. Для імітації одного дня T становить 86400 секунд, а в ідеалі βt - 600 секунд. Середня кількість транзакцій на блок βTx можна розрахувати як:

де Txday – кількість транзакцій за день, які можна обчислити за наступною формулою:

Коефіцієнт надходження λ(s) можна розрахувати як:

де Uday – кількість непідтверджених транзакцій на кінець кожного дня:

Uday = Countmempool + Countminingpool – Uday-1

А середній час майнінгу μ(s) розраховується як:

де, m – кількість майнерів в видобувному пулі.

**Схема і граф станів системи масового обслуговування.**

На рисунку 4 представлена запропонована модель нашої системи блокчейн; Ми розглядаємо пул пам'яті як єдину чергу з одним сервером, а пул майнінгу з кількома номерами серверів або майнерів, як правило, на кілька більше, ніж розмір блоку. Однак справжня мережа блокчейн складається з сотень мільйонів користувачів і майнерів, та запропонована модель також може бути масштабована для цієї мети. Але для простоти розуміння ми вибрали найпростішу модель для описання. Пул пам'яті налаштовується за допомогою M/M/1, а майнінг-пул з чергою M/M/c. Майнінг-пул розміщується між набором станцій Fork і Join. Вилка використовується для двох цілей; Перший полягає в тому, щоб накопичити транзакції для управління заданим розміром блоку заnd раз, а другий - генерувати потоки, які будуть видобуватися кількома майнерами паралельно. Ємність форка обмежується одним розміром блоку, як тільки досягається необхідна кількість транзакцій. Кожна транзакція перетворюється в один потік (однак, потоків для однієї транзакції може бути багато) і передається в пул майнінгу, де ряд майнерів з пулу можуть отримати потоки для виконання операції майнінгу на всіх потоках одночасно. Після завершення майнінгу всі транзакції повинні бути приєднані до станції, де всі потоки блоку накопичуються, утворюючи блок, який потім перенаправляється в мережу.

VFK

Для досягнення ідеального часового проміжку між блоками майнінг-пул налаштовується на стандартній час, еквівалентний 600 секундам для майнінгу кожного блоку. Наприклад, якщо у блоці 2000 транзакцій, то середній час майнину займатиме 600 секунд. Якщо у пулі знаходитиметься 2100 вузлів-майнерів, то сервісний час майнингу можна розрахувати як: .

2000

Форк-станція налаштована з кінцевою ємністю для розміру блоку, надлишкові транзакції будуть відкинуті, а в мережі Blockchain пакет або транзакція не будуть втрачені через трансляцію вхідних транзакцій в кілька вузлів однорангової мережі. Щоб подолати проблему втрати транзакцій в нашій моделі, ми використовували правило Block After Service (BAS) на форк-блоку, так якщо кількість транзакцій вже досягла розміру блоку b, пул пам'яті не зможе відправити подальші транзакції ; натомість ці транзакції накопичуються в пулі пам'яті.

У нашій запропонованій моделі ми використовували політику a first-come-first-serve (FCFS) для моделювання всіх етапів, включаючи пул пам'яті, розгалуження та майнінг-пул. Однак політика масового обслуговування може бути змінена під конкретний тип моделювання. Надходження транзакцій слідує за розподілом Пуассона, і після майнінгу та приєднання транзакцій блок транзакцій видаляється з системи.

**Комп’ютерна програма мовою Python.**

**Аналіз результатів**

**Висновок**