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 вузли мережі P2P підтримують свою власну копію блокчейну, відому як леджер.

Основним протоколом криптовалюти біткойн є консенсус, який вимагає, щоб усі однорангові вузли погоджувалися щодо кожного окремого запису блоку в розподілений блокчейн. Останнім часом блокчейни привернули величезну увагу кількох інститутів. 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 виправданою, 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 – Пропускна здатність біткоїна непорівнянно менша ніж у платіжної системи Visa.

Математичний опис моделі

Як зображено на рисунку 1, 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);

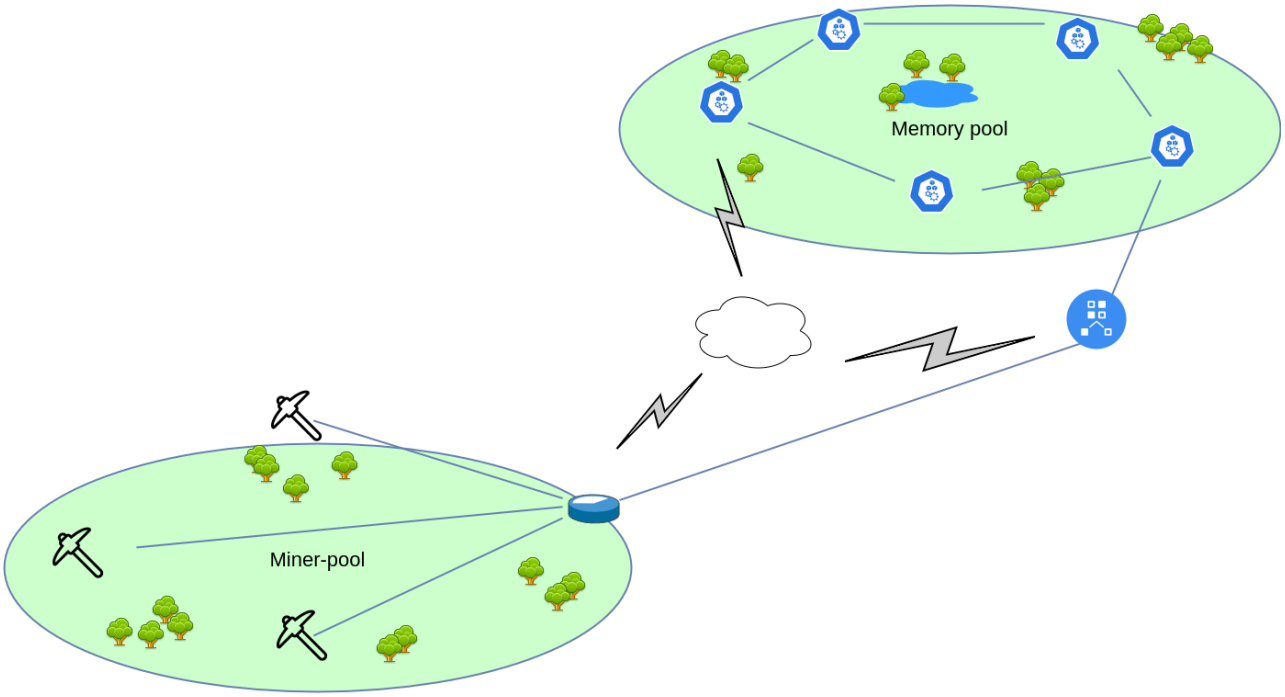


Рисунок 1

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 то 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, β_n, можна розрахувати за допомогою:

$$\beta_n = \frac{T}{\beta_t}$$

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

$$\beta_{Tx} = \frac{Tx_{day}}{\beta_n}$$

де Tx_{day} – кількість транзакцій за день, які можна обчислити за наступною формулою:

$$Tx_{day} = \frac{Tx}{sec} \times T$$

Коефіцієнт надходження $\lambda_{(s)}$ можна розрахувати як:

$$\lambda_{(s)} = \frac{Tx_{day} + U_{day}}{T}$$

де U_{day} – кількість непідтверджених транзакцій на кінець кожного дня:

$$U_{day} = Count_{mempool} + Count_{miningpool} - U_{day-1}$$

А середній час майнінгу $\mu_{(s)}$ розраховується як:

$$\mu_{(s)} = \frac{\beta_{Tx} \div 600}{m}$$

де, m – кількість майнерів в видобувному пулі.

Схема і граф станів системи масового обслуговування.

На рисунку 2 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 этапів Fork і Join. Fork використовується для двох цілей; Перша полягає в тому, щоб накопичити транзакції для управління заданим розміром блоку та його розміру, а другий – генерування потоків, які будуть видобуватися кількома майнерами паралельно. Ємність форка обмежується одним розміром блоку, форк готовий 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 отримують потоки для виконання операції майнінгу одночасно. Після завершення майнінгу всі транзакції потрапляють на етап Join, де всі потоки блоку накопичуються, утворюючи блок, який потім перенаправляється в мережу.

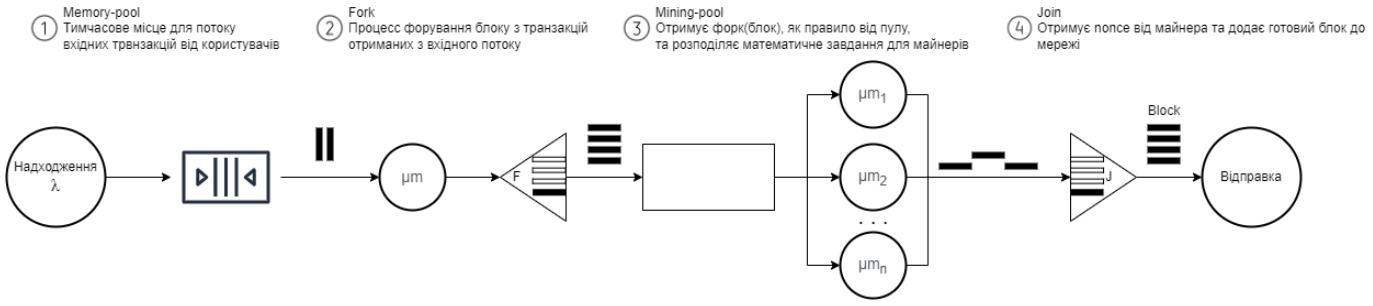


Рисунок 2

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: $\frac{2100/600}{2000} = 0.0015873$.

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, форк 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

Створимо деякий клас, який буде характеризувати нашу систему масового обслуговування у сфері електронних платежів, на основі блокчейну.

```
class BC_Simulation:
  def __init__(self):
    self.clock=0.0                #simulation clock
    self.transaction_arrivalrate = 3.432

    self.transactions_dispatched = 0.2941
    self.initial_mempool_transactions = 5641
    self.queue_capacity = np.Infinity
    self.mempool_size = self.initial_mempool_transactions

    self.transaction_count = 0
    self.block_count = 1

    self.mining_rate = np.arange(0.001546, 0.001650)
    self.miners_count = 2000

    self.block_size = 1024
    self.transaction_weight = 0.5
    self.mining_time = 600
```

Додомо деякі функції, що будуть імітувати роботу нашого блокчейну. Так як у попередній лабораторній роботі, де ми дослужували надходження блоків до мережі, та зробили висновок що надходження є точковим пуассонівським процесом, тому будемо моделювати саме за розподілом пуассона.

```
def add_mempool(self):
        self.mempool_size += self.mining_time * np.random.uniform(low=0.01,high=1.8)  *
 np.random.poisson(self.transaction_arrivalrate)
        print(int(self.mempool_size),np.random.poisson(self.transaction_arrivalrate))
        return self.mempool_size

    def fork(self):
        fork = 0
        self.transaction_count = 0
        while(self.block_size > fork):
            self.transaction_count += 1
            fork += (self.transaction_weight * np.random.uniform(low=0.01,high=1.8))
        print(fork, self.transaction_count)

        if(self.mempool_size < self.transaction_count):
            self.mempool_size = 0
        else:
            self.mempool_size = self.mempool_size - self.transaction_count
        return self.transaction_count

    def miningpool(self):
        i = 0
        nonce = 0
        while self.miners_count > i:
            i += 1
            nonce += np.random.uniform(0.001546, 0.001650)
        return(self.transaction_count / nonce )

    def join(self):
        print("ok")
```

Приклад одного з методів для побудови графіків для аналізу результатів.

```
def block_trns():
    plt.figure(figsize=(16,10), dpi= 80)
    plt.plot('Block_index', 'Transaction_in_block', data=df1, color='tab:red')

    # Decoration
    plt.ylim(50, 4000)
    xtick_location = df1.index.tolist()[::12]

    plt.xticks(ticks=xtick_location,  rotation=0, fontsize=12, horizontalalignment='center', alpha=.7)
    plt.yticks(fontsize=12, alpha=.7)
    plt.title("Кількість транзакцій у блоці", fontsize=22)
    plt.grid(axis='both', alpha=.3)

    # Remove borders
    plt.gca().spines["top"].set_alpha(0.0)
    plt.gca().spines["bottom"].set_alpha(0.3)
    plt.gca().spines["right"].set_alpha(0.0)
```

```
plt.gca().spines["left"].set_alpha(0.3)
plt.show()
```

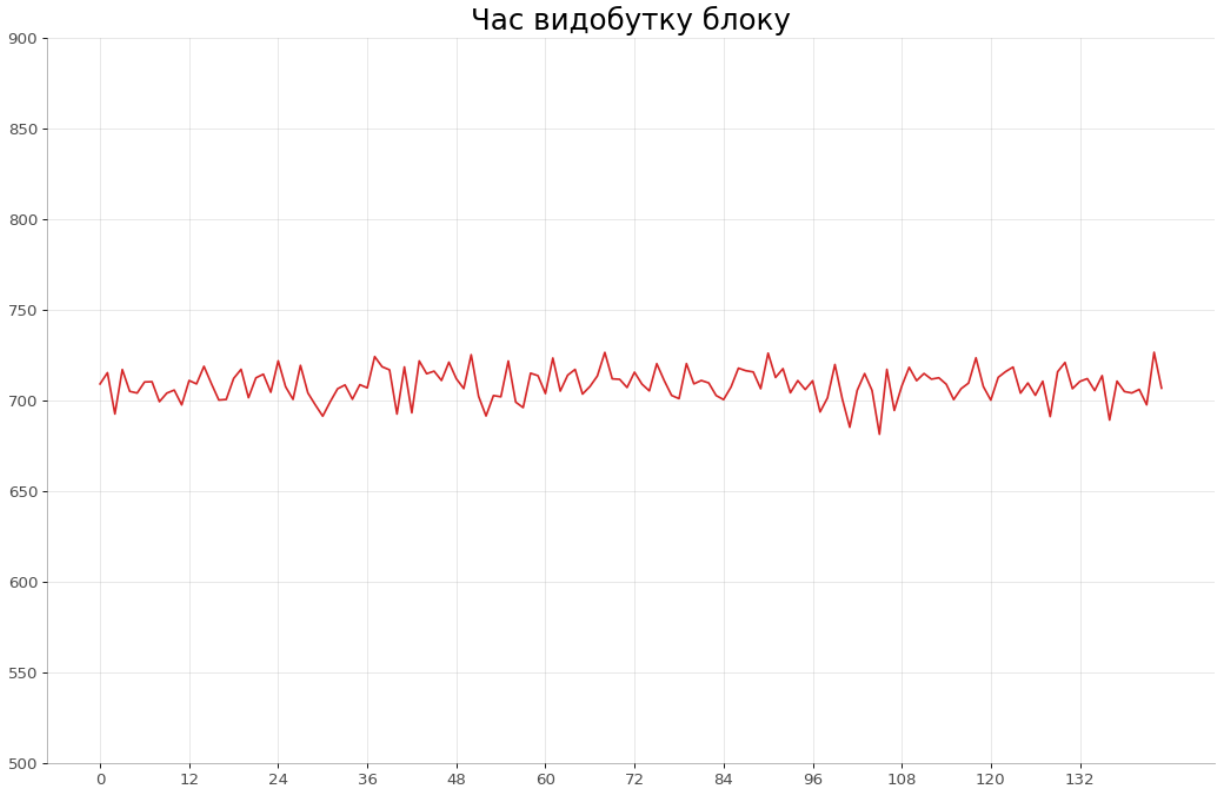
Аналіз результатів

Метою цього дослідження є вперше створити імітаційну модель для вивчення поведінки системи блокчейн за допомогою теорії масового обслуговування. Запропонована модель застосовна до малих і великомасштабних систем, а також для коротко- і довгострокового моделювання будь-якої такої системи. У цьому розділі ми представляємо результати короткострокового моделювання криптовалюти Bitcoin за один день. Результати наведено на малюнках 3 - 6 узагальнюючи спостереження під час одноденних транзакцій з криптовалютою Bitcoin. Моделювання було виконано з параметрами, зазначеними в таблиці 1. Важливі індекси, які розглядає Bitcoin explorer для оцінки повсякденних транзакцій, отриманих із запропонованої моделі імітації. Показники продуктивності, показані на малюнках 3 - 6: (3) Кількість транзакцій на блок (4) Час майнінгу кожного блоку (5) Кількість транзакцій за секунду (6) Кількість пулів пам'яті та кількість непідтверджені транзакції у всій системі.

1. Кількість транзакцій на блок

Згідно з ідеальними теоретичними припущеннями про біткойн, кількість транзакцій на блок не повинна перевищувати обмеження розміру в 1 МБ, і, як описувалося раніше, ми припустили, що існує 2100 Tx/блок. Однак тенденція на

малюнку 3 показує, що перший блок починається з 2200 транзакцій, а потім збільшується, в момент, коли система стає стабільною та забезпечує 2300 для решти згенерованих блоків.

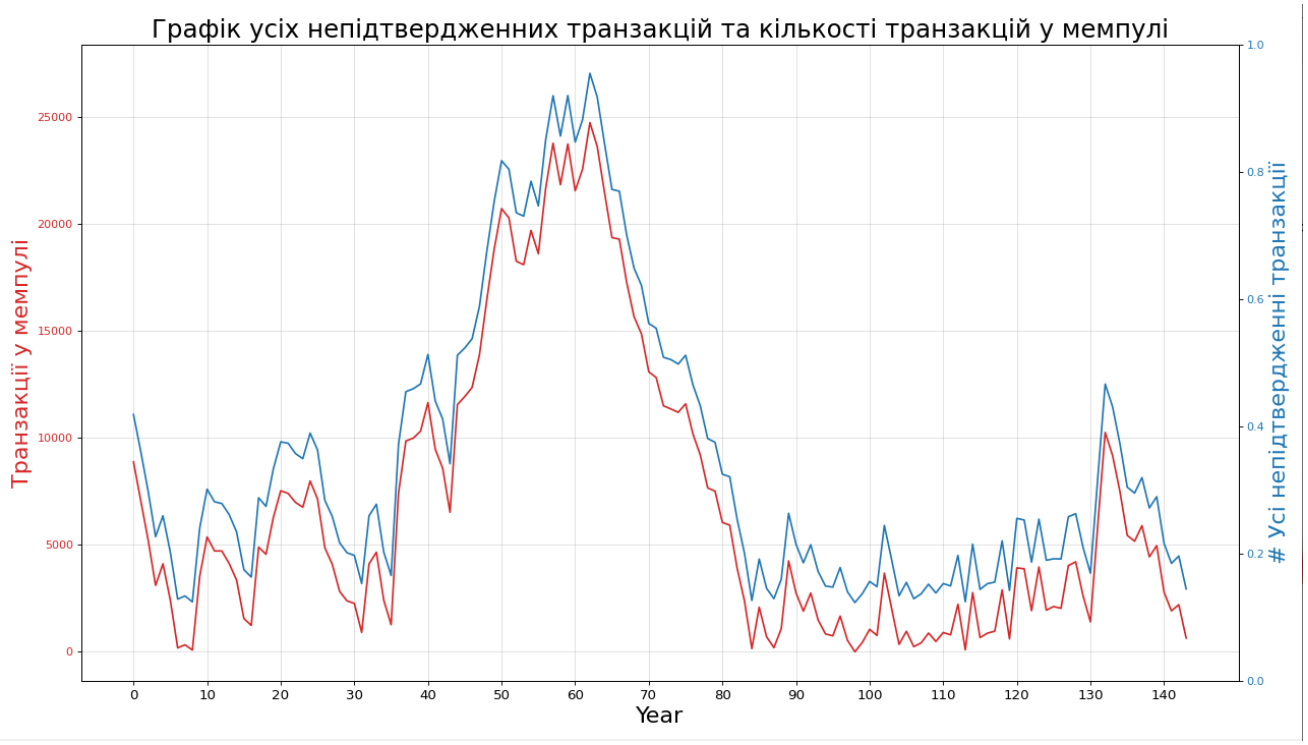


2. Час майнінгу кожного блоку.

У попередньому розділі ми ознайомитилися з жорстко закодованими правилами блокчейну, які передбачають, що в ідеалі майнеру для виявлення блоку потрібно приблизно 10 хвилин (або 600 секунд). Однак це часове обмеження не може бути точно дотримано в реальних ситуаціях; час видобутку завжди різниться, і один блок відрізняється від іншого з точки зору складності видобутку. На цьому графіку ми бачимо, що час видобуток блоку залежить від блоку до блоку, що дуже реалістично. Коливання часу майнінгу становили від 687 до 742 с, а середній час майнінгу за весь день становить 600 с/блок.

3. Кількість транзакцій за секунду

Кількість підтверджених транзакцій за секунду на блок, або пропускна здатність системи, є найбільш критикованим параметром біткойна, коли справа доходить до порівняння його з Visa та іншими платіжними системами. На цьому графіку показано середню кількість підтверджених транзакцій за секунду на блок, що означає час, який знадобився для успішного підтвердження транзакції.



4. Mempool Count

Ми припустили, що кількість надходжень до системи трохи більше, ніж тих, що обслуговуються на станції майнінгу. Наприклад, якщо кількість транзакцій, що надходять до системи, становить 3,55/с, а загальна потужність майнінгу становить 3,5, то в якийсь момент транзакції почнуть накопичуватися в Mempool. Це впливає на систему Bitcoin, і кількість накопичених непідтверджених транзакцій зростає протягом дня.

5. Кількість непідтверджених транзакцій у всій системі

Надходження транзакцій за день є непередбачуваним; в певний момент може бути велика кількість транзакцій, що надходять в систему, тоді як в наступний момент кількість надходжень може бути меншою, ніж зазвичай.

Таким чином, вхідні запити на транзакції від користувачів не є фіксованими, а час обробки та потужність системи мають кілька обмежень, що змушує систему поводитися певним і встановленим способом, тобто обробка системи не залежить від навантаження. У нашому моделюванні було встановлено, що кількість надходжень буде трохи вищою, ніж необхідно, тобто від тих, що очікують у підрахунку Mempool, хоча це не єдині транзакції, присутні в системі в певний час. Процес майнінгу біткойнів ніколи не переходить у стан очікування; тому ми можемо сказати, що в будь-який момент часу на форк накопичується певна кількість транзакцій, і деякі з них чекають розповсюдження на етапі Join, щоб завершити процесс підтвердження блоку.

Транзакції всередині MiningPool та MemPool разом відповідають кількості непідтверджених транзакцій у всій системі. Цей індекс продуктивності зазвичай не обговорюється в статистиці біткойн, але це один із найважливіших факторів, який також слід враховувати при оцінці будь-якої системи побудованої на основі блокчейну.

Висновок

Блокчейни залишаються відносно невивченими для теоретичного моделювання. У цій роботі ми пропонуємо модель для симуляції блокчейну з використанням теорії масового обслуговування. Запропонована модель побудована з використанням однієї черги M/M/1 як пулу пам’яті, набору fork-join для пакетної генерації та черги M/M/c як пулу майнінгу. Запропонована модель є простим, але потужним засобом для виявлення багатьох важливих показників, таких як

- Кількість транзакцій на блок
- Час майнінгу кожного блоку
- Пропускна здатність системи/транзакцій за секунду (d) кількість пулу пам’яті
- Час очікування в пулі пам’яті
- Кількість непідтверджених транзакцій у всій системі

- Загальна кількість транзакцій та
- Кількість згенерованих блоків.

По-перше, запропонована модель була використана для оцінки ідеальної статистики транзакцій за один день у мережі Біткоїну. А потім модель використовувалася для симуляції фактичної статистики біткойну. Отримані результати добре узгоджуються з фактичними показниками, з незначним відсотком похибок. Незважаючи на те, що запропонована модель використовується для оцінки криптовалют у цій роботі, вона все ще здатна імітувати різноманітні системи на основі блокчейну для оцінки продуктивності та оптимізації систем.