МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра програмних систем і технологій

**Курсова робота**

на тему

“Розробка блокчейн вузла у якості автоматизованої системи безготівкових платежів”

Виконав: ст. гр. ІПЗ-33

Гоша Давід

Керівник практики:

д.т.н. с.н.с Порєв Геннадій Володимирович

Київ – 2023

# **Анотація**

У цій курсовій роботі представлено документ архітектури програмного забезпечення (SAD) для нової платіжної системи на основі блокчейну, що має на меті подолання обмежень існуючих технологій. Описано архітектуру запропонованої системи, дизайн інтерфейсу користувача та деталі реалізації. У статті також досліджується механізм надходження блоків і виявляється, що він підпорядковується пуассонівському розподілу, що призводить до парадоксу в часі підтвердження транзакцій. В цілому, стаття пропонує детальний план вдосконалення системи електронних платежів за допомогою технології блокчейн.

# **Вступ**

У сфері технології блокчейн та її застосувань, що постійно розширюється, одним з найважливіших питань, що викликають інтерес, є її потенціал для революційної перебудови платіжних систем. Однак, існуючі моделі стикаються з рядом обмежень і проблем, які перешкоджають їх широкому впровадженню і використанню. Ця курсова робота мотивована необхідністю вирішення цих проблем, прокладаючи шлях до більш ефективної та надійної платіжної системи на основі блокчейну.

Основною метою даної роботи є дослідження та розробка прототипу системи, яка перевершує існуючі аналоги в критичних аспектах. Ця система покликана забезпечити вирішення загальних проблем, що спостерігаються в поточних проектах, таких як масштабованість, швидкість транзакцій, енергоспоживання і безпека, тим самим демонструючи інноваційний підхід в середовищі блокчейн-технологій.

У цій роботі досліджується науковий процес моделювання та експериментів для демонстрації переваг запропонованого прототипу системи. У ній зроблена спроба розробити відповідний критерій для формалізації поліпшень системи, виміряних за допомогою конкретних метрик, таким чином забезпечуючи науковий результат, який обґрунтовує запропоновані рішення.

Усуваючи виявлені прогалини в існуючих системах і пропонуючи реалістичні рішення, це дослідження сподівається зробити значний внесок у сферу технології блокчейн. Потенційний вплив цих удосконалень охоплює більш ефективну систему транзакцій, підвищену масштабованість, посилену безпеку і зниження енергоспоживання, що розширює межі можливого на сьогоднішній день.

Ця робота складається з основних розділів, в яких розглядаються основні концепції технології блокчейн, дослідницький підхід, математичне моделювання системи та програмна реалізація прототипу. Наприкінці наводяться підсумки отриманих результатів та їх значення в більш широкому контексті платіжних систем на основі блокчейну.

## **1.1 Мета роботи**

Метою цього науково-дослідного проекту є вирішення та пом'якшення деяких існуючих проблем, що існують в сучасному ландшафті платіжних систем, заснованих на блокчейні. Ця ініціатива зумовлена прагненням підвищити стійкість, надійність і продуктивність цих систем шляхом впровадження інноваційної концепції станів у блокчейні та гібридного механізму консенсусу.

Основною метою є проектування і розробка прототипу системи, яка включає в себе ці вдосконалення. Через процес ретельного дослідження, формулювання концепції, розробки програмного забезпечення та ретельного тестування ми прагнемо створити платіжну систему на основі блокчейну, яка значно зменшить затримку транзакцій та омине проблеми централізації, що часто асоціюються з новими впровадженнями блокчейну.

Особливість нашого проекту полягає в підході до використання гібридного механізму консенсусу - інновації, що поєднує в собі докази роботи (PoW) і докази часу, що минув (PoET). Ця комбінація обіцяє підтримувати децентралізацію, забезпечуючи при цьому ефективну перевірку транзакцій - баланс, якого виявилося складно досягти в існуючих системах блокчейн.

Це дослідження має важливе значення в той час, коли технологія блокчейн широко впроваджується в різних секторах. Розглядаючи властиві їй проблеми і пропонуючи можливі рішення, ця робота прагне зробити істотний внесок у цю галузь, сприяючи використанню більш надійних, ефективних і справедливих систем блокчейн в реальних додатках.

## **1.2 Актуальність дослідження**

В останні роки популярність криптовалют зростає в геометричній прогресії. Однак, оскільки індустрія продовжує розширюватися, проблеми, пов'язані з існуючими технологіями, стають все більш очевидними. Основними проблемами сучасного ринку є високі транзакційні витрати в таких мережах, як Ethereum, та значні затримки транзакцій в таких мережах, як Bitcoin. Актуальність цього дослідження полягає в тому, що в ньому розглядається новий підхід до вирішення цих проблем, що значно підвищує продуктивність і покращує користувацький досвід платіжних систем, заснованих на блокчейні.

Крім того, зростаюче занепокоєння у криптовалютному просторі викликає централізація мереж у майнінг-пули. Така централізація підриває одну з фундаментальних філософій технології блокчейн - децентралізацію. Запропонований у цьому дослідженні гібридний протокол консенсусу має на меті вирішити цю проблему, сприяючи децентралізації та підвищенню безпеки і надійності блокчейну.

Це дослідження є не тільки своєчасним, але й дуже актуальним, оскільки воно пропонує потенційні рішення поточних проблем і робить свій внесок у дискусію про майбутній розвиток технології блокчейн. У зв'язку зі стрімким зростанням і все більшим поширенням криптовалют, потреба галузі в більш ефективному, надійному і децентралізованому рішенні стає все більш нагальною.

Ця робота потенційно може змінити поточне середовище технології блокчейн, розширити межі можливого і прокласти шлях до нового покоління криптовалют. Отримані результати можуть вплинути на розвиток майбутніх проектів і відкрити нові напрямки досліджень у цій захоплюючій і швидкозростаючій галузі.

## **1.3 Порівняння аналогів**

У цьому дослідженні пропонується новий гібридний протокол консенсусу, який намагається обійти ключові проблеми, що спостерігаються в наступних аналогах.

* **Litecoin**: однорангова криптовалюта, Litecoin була розроблена як "полегшена версія Bitcoin". Вона має на меті обробляти блок кожні 2,5 хвилини (порівняно з 10 хвилинами у Біткоїна) і забезпечує більш швидке підтвердження транзакцій. Однак, як і Біткоїн, вона використовує алгоритм консенсусу Proof-of-Work (PoW), що може призвести до збільшення споживання енергії та затримки транзакцій у сценаріях з високим трафіком. На противагу цьому, запропонована нами система зменшує споживання енергії завдяки використанню гібридного протоколу консенсусу.
* **Dogecoin**: В основному використовується для отримання чайових в інтернеті, Dogecoin також використовує алгоритм PoW. Хоча він має швидший час обробки блоків, ніж Bitcoin і Litecoin, його залежність від PoW все ще викликає занепокоєння щодо масштабованості та енергоспоживання.

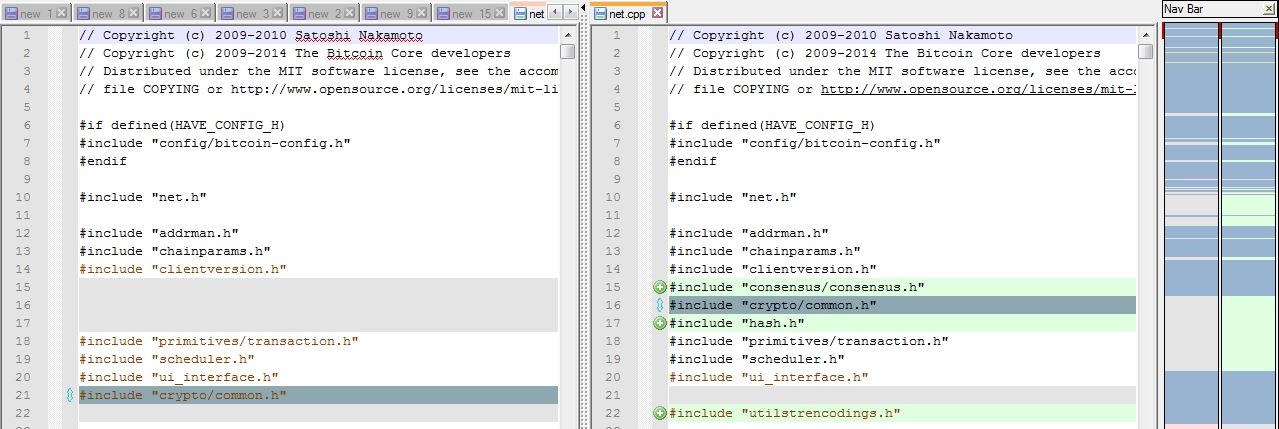


Рисунок 1 Порівняння вихідного коду net.cpp (ліворуч Dogecoin, праворуч Bitcoin)

* **Ethereum**: Будучи другою за величиною криптовалютою, Ефіріум запровадив концепцію смарт-контрактів. Тим не менш, Ethereum стикається з проблемами масштабованості і піддається критиці за високу комісію за транзакції. Мережа Ethereum також використовує консенсус PoW, що призводить до подібних проблем зі споживанням енергії та затримкою транзакцій. Ці проблеми вирішуються в запропонованій нами системі за допомогою гібридного протоколу консенсусу, спрямованого на зниження транзакційних витрат і поліпшення масштабованості.
* **Solana**: Solana - це високопродуктивний блокчейн, який обіцяє швидкі та безпечні децентралізовані додатки та криптовалюти. Він використовує унікальну систему міток часу під назвою Proof of History (PoH) в поєднанні з механізмом консенсусу PoS (Proof of Stake). Однак, були висловлені занепокоєння з приводу централізації мережі. Запропонована нами система націлена на вирішення цієї проблеми, забезпечуючи децентралізацію за допомогою гібридного протоколу консенсусу.
* **Cardano**: Cardano використовує унікальний алгоритм PoS під назвою Ouroboros, який є менш енергоємним, ніж PoW. Хоча він пропонує більш енергоефективну альтернативу Ethereum, мережа все ще стикається з проблемами швидкості транзакцій і масштабованості. Запропонована нами система має на меті покращити ці аспекти за допомогою гібридного механізму консенсусу.
* Polygon: Polygon - це фреймворк для створення та підключення сумісних з Ethereum блокчейн-мереж. Вона спрямована на усунення обмежень Ethereum, включаючи пропускну здатність, поганий користувацький досвід (висока швидкість і затримка транзакцій) і відсутність суверенітету для розробників. Однак деякі критики вказують на можливі проблеми з централізацією та безпекою, пов'язані з моделлю консенсусу PoS.

Підсумовуючи, можна сказати, що хоча кожна з вищезгаданих платформ зробила цінний внесок у цю галузь, вони також стикаються з певними проблемами - такими як енергоефективність, затримка транзакцій, масштабованість і централізація. Запропонована нами система має на меті вирішити ці проблеми шляхом прийняття нового гібридного протоколу консенсусу. Цей підхід дозволяє нам використовувати сильні сторони існуючих систем, одночасно покращуючи їх слабкі сторони, обіцяючи ефективну, масштабовану і по-справжньому децентралізовану платіжну систему на основі блокчейну.

# **2. Теоретична інформація**

У цьому розділі викладено теоретичні основи, що стосуються нашого дослідження, пропонуючи всебічний огляд існуючих технологій блокчейн і їх застосування, з подальшим вивченням гібридного протоколу консенсусу. Ці елементи забезпечують базові знання, необхідні для розуміння природи досліджуваної проблеми, запропонованого рішення і унікальних аспектів розробленої системи.

## **2.1 Існуючі технології блокчейн та їх застосування**

Технологія блокчейн, з моменту її появи з біткоїном, зробила революцію в тому, як проводяться транзакції та зберігаються записи в децентралізованому, безпечному режимі. Однак система блокчейну значно еволюціонував, і нові технології пропонують унікальні підходи до масштабованості, безпеки та різноманітності застосувань.

1. Біткоїн: Піонер технології блокчейн, біткоїн, представив концепцію децентралізованих цифрових валют. Він спирається на механізм консенсусу Proof-of-Work (PoW) для підтвердження і запису транзакцій. Успіх біткоїна вплинув на наступні технології блокчейну, але він також має недоліки, пов'язані, насамперед, з масштабованістю та швидкістю транзакцій.
2. Ефіріум: Ethereum розширив концепцію блокчейну за межі простих транзакцій, запровадивши програмовані смарт-контракти. Це сприяло розвитку децентралізованих додатків (DApps) та первинних пропозицій монет (ICO). Однак Ethereum, як і Bitcoin, стикається з проблемами масштабування та високими комісіями за транзакції.
3. Litecoin і Dogecoin: спочатку представлені як альтернатива біткоїну, Litecoin і Dogecoin пропонують швидший час генерації блоків, тим самим прагнучи забезпечити швидке підтвердження транзакцій. Однак, швидший час створення блоків може призвести до більшої ймовірності розгалуження.
4. Cardano: Cardano пропонує унікальну дворівневу архітектуру для відокремлення реєстру значень рахунків від причини, по якій значення переміщуються з одного рахунку на інший. Це розділення має на меті покращити функціональність смарт-контракту. Механізм консенсусу - Proof-of-Stake (PoS), який вважається більш енергоефективним, ніж PoW.
5. Solana: Solana впроваджує нову систему міток часу для підвищення ефективності мережі, яка має на меті обробляти тисячі транзакцій в секунду. Однак були висловлені занепокоєння щодо централізації.
6. Polygon (Matic): Як рішення для масштабування поза ланцюжком для Ethereum, Polygon забезпечує швидші та дешевші транзакції. Тим не менш, були виявлені проблеми з безпекою, пов'язані з його механізмом вибору валідатора.

З точки зору застосування, технології блокчейн розгортаються у сферах, що виходять далеко за межі криптовалют. Децентралізовані фінанси (DeFi), відстеження ланцюжків поставок, цифрова ідентифікація особи, системи голосування та не взаємозамінні токени (NFT) - це лише кілька прикладів трансформаційного потенціалу технологій блокчейн.

Ці технології дають цінну інформацію та слугують важливими орієнтирами для розробки запропонованої платіжної системи, яка має на меті поєднати сильні сторони та пом'якшити недоліки існуючих рішень. Наступний розділ присвячений одному з таких інноваційних підходів: гібридному протоколу консенсусу.

## **2.2 Proof-Of-Work**

У цьому розділі обговорюється реалізація консенсусу в системі блокчейн Біткоїн. Сатоші Накамото у своєму документі про Біткоїн посилався на систему Hashcash Адама Бека, яка вперше представила алгоритм Proof of Work (PoW) як універсальну технологію захисту від спаму.

Концепція, що лежить в основі, проста: Якщо вузол повинен виконати певну обчислювальну роботу, перш ніж підтвердити блок, йому буде невигідно атакувати мережу тисячами транзакцій в секунду. Хоча ця технологія може використовуватися в інших системах для запобігання спаму, в контексті Біткоїна консенсус відіграє життєво важливу роль у рівномірному розподілі емісії монет і виборі лідера для додавання нового блоку до блокчейну.

Біткоїн використовує алгоритм хешування SHA-256. Він бере набір транзакцій у блоці і повертає 256-бітний хеш. Встановивши правило, що мережа прийматиме хеш лише з певною кількістю початкових нулів, можна збільшити складність пошуку відповідного хешу. Відповідно, це зменшує діапазон прийнятних хешів і збільшує час, необхідний для хешування.

Щоб гарантувати, що однакові вхідні дані не завжди дають однаковий хеш, було введено поняття, яке називається "nonce". Подаючи випадкові дані (nonce) разом з транзакціями на функцію хешування, можна згенерувати різні хеші для одного і того ж блоку. Вузли будуть продовжувати хешування з різними nonce до тих пір, поки один з них не знайде хеш в прийнятному діапазоні.

Обчислювальна потужність мережі, яка залежить від кількості вузлів-учасників, є динамічною. Якщо кількість майнерів подвоюється, швидкість підтвердження блоків також подвоюється, що прискорює процес підтвердження, але потенційно призводить до збільшення навантаження на мережу і швидкості емісії монет. Щоб запобігти цьому, мережа коригує рівень складності приблизно кожні 2016 блоків, або приблизно кожні два тижні, щоб підтримувати середній час підтвердження блоку на рівні 10 хвилин.

Форки, або розгалуження в блокчейні, можуть виникати, коли два різних блоки одночасно знаходять правильний хеш. У цій ситуації мережа фактично розділяється на дві частини, кожна з яких продовжує свою гілку. Ця проблема вирішується дотриманням правила "найдовший ланцюжок перемагає": та гілка, яка першою додає наступний блок, визнається головною гілкою. Вузли, які працювали на коротшій гілці, повинні перейти на нову головну гілку. Тому для забезпечення підтвердження транзакції важливо дочекатися більш ніж одного підтвердження від мережі.

## **2.3 Proof-Of-Elasped-Time**

Proof of Elapsed Time (PoET) - це алгоритм консенсусу, який використовується в системах блокчейн, зокрема на платформі Intel Sawtooth Lake. PoET розроблений для забезпечення справедливого і високомасштабованого процесу підтримки консенсусу в децентралізованій мережі, при цьому пом'якшуючи деякі з істотних проблем споживання ресурсів, пов'язаних з іншими алгоритмами консенсусу.

Основа PoET відносно проста. Мета полягає в тому, щоб визначити легітимність і порядок транзакцій в децентралізованій системі, що є критично важливим для будь-якої мережі блокчейн. Замість того, щоб покладатися на величезні обчислювальні потужності, як в Proof of Work (PoW), або володіння великою часткою в мережі, як в Proof of Stake (PoS), PoET використовує систему випадкової лотереї для вибору вузла, який додає наступний блок до ланцюжка.

В алгоритмі PoET кожен вузол, що бере участь в мережі, генерує випадковий час очікування і засинає на цей час. Вузол, який прокидається першим - тобто вузол з найкоротшим часом очікування - додає новий блок до блокчейну і транслює його решті мережі. Цей процес повторюється для додавання кожного нового блоку. Це наче кожен вузол - поет, який чекає на натхнення; той, хто прокинеться першим, напише наступний рядок "поеми", якою є блокчейн.

Критично важливим аспектом PoET є забезпечення цілісності часу очікування. Для цього PoET використовує розширення Intel Software Guard Extensions (SGX), які дозволяють програмам запускати надійний код у захищених контейнерах, відомих як анклави. SGX гарантує, що код, який генерує випадковий час очікування і спить протягом цього часу, працює, як очікувалося, і не був підроблений, тим самим забезпечуючи чесність лотерейної системи.

PoET має кілька переваг як алгоритм консенсусу. Він є енергоефективним, оскільки вузлам не потрібно виконувати обчислювально інтенсивні завдання, і вони можуть переходити в режим сну з низьким енергоспоживанням під час очікування. PoET також підтримує високий ступінь масштабованості, оскільки додавання нових вузлів до мережі не призводить до значного збільшення обчислювальної потужності, необхідної для досягнення консенсусу. Нарешті, PoET сприяє справедливості, оскільки кожен вузол, незалежно від його обчислювальної потужності або частки в мережі, має рівні шанси бути обраним для додавання наступного блоку.

Незважаючи на ці переваги, з PoET пов'язані також проблеми і критика. Він покладається на надійне середовище виконання, надане Intel SGX, що викликає занепокоєння щодо централізації та довіри. Крім того, він може стати вразливим, якщо зловмисник знайде спосіб скомпрометувати SGX або маніпулювати процесом генерації випадкових чисел.

На закінчення, Proof of Elapsed Time представляє унікальний та інноваційний підхід до питання консенсусу в мережах блокчейн. Поєднуючи елементи випадковості, справедливості та енергоефективності, він означає значний відхід від традиційних механізмів консенсусу, що вимагають значних ресурсів. Однак, як і всі технології, вона не позбавлена потенційних проблем і повинна постійно перевірятися, тестуватися і розвиватися, щоб зменшити будь-які вразливості і підтримувати цілісність систем, які вона підтримує.

## **2.4 Майнінг**

Майнінг нерозривно пов'язаний з механізмом консенсусу щодо доказів роботи. Через відсутність центрального органу влади в мережі за замовчуванням виникає проблема, відома як "проблема візантійських генералів". Це класичний виклик в криптографії, що передбачає прийняття рішень в потенційно ворожому середовищі. У Біткоін вона вирішується шляхом випадкового вибору вузла, блок якого визнається дійсним всією мережею.

По суті, учасники мережі, включаючи майнерів, грають у своєрідну криптографічну лотерею. Вони перевіряють цілісність блоку, порівнюючи його хеш з хешами інших вузлів; якщо в блоці є навіть незначні зміни, хеш буде кардинально відрізнятися, що робить подальші зусилля з майнінгу марними, оскільки мережа відхилить такий блок.

Після перевірки блоку всі учасники намагаються знайти відповідний хеш за допомогою nonce. Як тільки такий хеш знайдено, успішний вузол отримує винагороду від бази монет і право додавати та розповсюджувати новий блок. Враховуючи, що пошук відповідного хешу є обчислювально інтенсивним завданням, майнеру, як правило, невигідно намагатися обдурити мережу; будь-які спроби змінити дані блоку, швидше за все, будуть помічені іншими вузлами, які потім відхилять блок майнера.

База монет - це спеціальна сутність в блокчейні, яка не має приватного ключа. Вона служить для виплати майнерам з власних резервів за їх внесок в мережу. База монет може бути відновлюваною або невідновлюваною.

У випадку з невідновлюваною базою монет

1. Майнер видобуває блок
2. Монетна база платить майнеру зі своїх резервів
3. Майнер також збирає частину комісії за транзакції

У випадку з відновлюваними монетними базами:

1. Майнер видобуває блок
2. Частина комісії за транзакції перераховується на монетну базу
3. Коін-чейн платить майнеру зі своїх резервів

Коли блок видобувається декількома майнерами одночасно, виникає конкуренція або "майнінгова гонка". Майнери з більшою обчислювальною потужністю мають більше шансів на перемогу. Однак координація цих зусиль для уникнення дублювання є складним завданням. Щоб вирішити цю проблему, створюються майнінг-пули, які об'єднують майнерів для роботи над однією проблемою і спільного використання ресурсів. Ці пули координують зусилля окремих майнерів, щоб вони не дублювали роботу один одного.

## **2.5 Баланс**

Топологія мережі, з якою ми маємо справу, є децентралізованою одноранговою, оскільки приклад, який ми розглядаємо, - це Біткоїн. Така мережева архітектура означає відсутність центральної точки управління. Така технологія породжує певні неоднозначні проблеми, такі як подвійні витрати. Проблема подвійних витрат була вирішена за допомогою ланцюжка цифрових підписів. Щоб зрозуміти це, нам потрібно абстрагуватися від традиційної моделі обміну фіатних грошей.

Біткоїн не має поля "баланс" або фізичних монет як таких. Існує лише один реєстр, який є ланцюжком усіх транзакцій. Звідси ми можемо математично визначити баланс вузла. По суті, це можна представити як ланцюжок передачі прав власності на частину загальної емісії валюти. Самі монети знаходяться в стані мономорфності і існують виключно для спрощення людського сприйняття. Підсумкове поле балансу користувача ніде не з'являється, ця величина є поліморфною.

При створенні наступної транзакції деякий сторонній вузол повинен перевірити реєстр - ланцюжок транзакцій, пов'язаних хешами попередніх транзакцій, щоб переконатися, що кількість входів більша або дорівнює кількості виходів. По суті, це перевірка, щоб підтвердити, чи має відправник достатньо коштів. Враховуючи, що один відправник може мати кілька вхідних і вихідних транзакцій, ми виводимо наступну формулу для визначення достовірності суми

переказу:

, де i = сума всіх вхідних переказів, o = сумою вихідних переказів

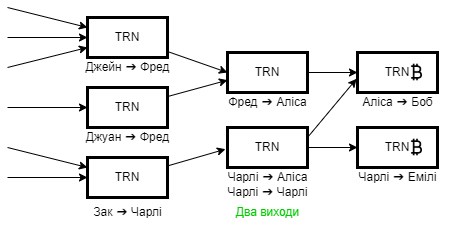


Рисунок 3 Спрощений ланцюжок транзакцій

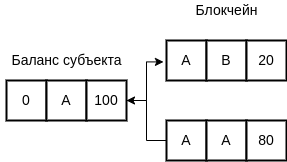
Блокчейн можна реалізувати різними способами, навіть якщо сфера застосування відома заздалегідь. Наприклад, якщо програма, що розробляється на основі блокчейну, є платіжною системою, то отримання балансу користувача вже може бути реалізовано двома способами: детермінованим і недетермінованим, не кажучи вже про склад блоку, обмеження блоку, винагороду за майнінг тощо. Така ситуація є більш негативною, оскільки безпека кінцевого продукту не буде визначатися загальноприйнятими стандартами, які пройшли відкритий і тривалий аналіз. Щоб протистояти цьому фактору, поширеною практикою є дотримання стандартів де-факто, таких як біткоїн (який діє як класична платіжна система) та Ethereum (який діє як платформа для смарт-контрактів).

## **2.6 Транзакції та UTXO модель**

Модель UTXO (Unspent Transaction Output) - це підхід до управління транзакціями без додаткової необхідності підтвердження права власності на кошти. Це означає, що при створенні переказу ми можемо розпоряджатися тільки всією частиною отриманих монет, пам'ятаючи про функціонал балансу. Оскільки фізичного поняття балансу не існує, це просто функція, яка рекурсивно відновлює кількість зобов'язань перед об'єктом по ланцюжку транзакцій. Таким чином, ви можете витратити залишок тільки повністю. Часткова витрата призведе до розгалуження гілок і неузгодженості в ланцюжку блокчейну. Механізм переказу монет працює наступним чином: об'єкт-відправник повинен переказати необхідну суму об'єкту-одержувачу, а якщо сума менша за залишок, то об'єкт повинен повернути залишок собі (див. рис. 2.1).

Вирішення проблеми подвійних витрат є дуже важливим. Враховуючи, що в мережі немає посередника або валідатора, якому за замовчуванням довіряють всі без винятку вузли, виникає проблема з прив'язкою транзакцій. Відправник A може відправити користувачеві B транзакцію, еквівалентну його балансу, а потім відправити таку ж суму користувачеві C. Мережа повинна мати певний алгоритм і ряд властивостей, щоб запобігти подібним типам атак. Для цього кожна транзакція містить посилання на попередню, тобто останню загальноприйняту на даний момент, і власний унікальний ідентифікаційний номер, який буде використовуватися для початку нових транзакцій в майбутньому. У Bitcoin такий ідентифікатор генерується за допомогою хешу самої транзакції і транзакції, формуючи таким чином спрямований список і захищаючи транзакцію від майбутніх змін.

Рисунок 3 Специфікація UTXO транзакції



Після цього транзакція потрапляє в пул пам'яті - місце, де вона вже потрапила в мережу, але ще не була записана в жодному з блоків, а отже, не була ефективно задекларована. Транзакція залишається в цьому стані до того моменту, поки її не буде додано до блоку. Блок - це колекція транзакцій розміром в один мегабайт. Блоки необхідні для оптимізації продуктивності мережі, оскільки підтвердження тисячі транзакцій одночасно є менш ресурсоємним і більш ефективним. Формування блоку починається зі створення реєстру - криптографічно підтвердженого впорядкування транзакцій, покликаного запобігти вразливості подвійних витрат. Після формування реєстру блок хешується за допомогою алгоритму дерева Меркла.

## **2.7 Вступ до гібридного протоколу консенсусу**

Технологія блокчейн базується на протоколах консенсусу, які визначають, як підтверджуються транзакції і як додаються нові блоки до блокчейну. Традиційно блокчейн-платформи використовують єдині механізми консенсусу, такі як Proof of Work (PoW) або Proof of Stake (PoS). Однак кожен з цих механізмів консенсусу має свої сильні і слабкі сторони, що викликає інтерес до гібридних підходів, які намагаються об'єднати найкращі характеристики обох.

Гібридний протокол консенсусу об'єднує різні механізми консенсусу з метою використання їхніх переваг і мінімізації недоліків. У цьому дослідженні ми зосередимося на гібридному протоколі, який поєднує в собі PoW і Proof of Elapsed Time (PoET).

* Доказ роботи (PoW): PoW - це оригінальний механізм консенсусу, запроваджений Біткоїном. У системі PoW майнери змагаються у вирішенні складної математичної задачі, і той, хто першим знайде рішення, отримує право додати наступний блок до блокчейну. Цей механізм забезпечує надійну безпеку, але є енергоємним і може призвести до збільшення часу виконання транзакцій.
* Підтвердження часу, що минув (PoET): PoET - це відносно новий механізм консенсусу, розроблений компанією Intel. Він розроблений як недорога, енергозберігаюча альтернатива PoW. У системі PoET мережа випадковим чином вибирає творця наступного блоку, виходячи з найменшого "часу очікування". Випадковість запобігає постійному додаванню нових блоків одним вузлом, тим самим заохочуючи децентралізацію.

Гібридний протокол консенсусу PoW/PoET має на меті отримати вигоду з безпеки і децентралізації PoW і енергоефективності та масштабованості PoET. Механізм працює таким чином, що PoW використовується для перевірки блоків, підтримуючи надійність системи. На противагу цьому, PoET використовується для створення блоків, забезпечуючи швидке і енергоефективне додавання блоків до ланцюжка.

Цей інноваційний протокол консенсусу є невід'ємною частиною дизайну і функціональності запропонованої платіжної системи, яка прагне вирішити проблеми масштабованості, швидкості транзакцій, енергоспоживання і централізації, які спостерігаються в існуючих технологіях блокчейн. Більш детальний аналіз того, як цей гібридний протокол консенсусу застосовується в архітектурі системи, представлений в розділі 5.1.

# **3 Ідентифікація проблеми**

У сфері технології блокчейн, незважаючи на те, що її інноваційний потенціал широко визнаний, існує чимало перешкод, які стримують її ефективність та швидкість впровадження. Поява цих проблем вимагає глибокого дослідження для розуміння їх першопричини, впливу та можливих рішень. Це має вирішальне значення для розвитку і прогресу систем на основі блокчейну, особливо в контексті платіжних систем, де ці проблеми можуть мати ще більший вплив.

У цьому розділі ми визначаємо і заглиблюємося в критичні проблеми, з якими наразі стикаються платіжні системи на основі блокчейну. Аналізуючи ці проблеми та їх наслідки, ми створюємо міцну основу для розробки нашого рішення, спрямованого на вирішення цих проблем, тим самим підвищуючи функціональність і зручність використання технології блокчейн в платіжних системах.

## **3.1 "Проблеми в платіжних системах на основі блокчейну"**

Незважаючи на інноваційний потенціал технології блокчейн, певні проблеми в існуючих платіжних системах на основі блокчейну обмежують їх ефективність та широке впровадження. У цьому розділі обговорюються ті ключові проблеми, на вирішення яких спрямований проект:

1. **Затримка транзакцій**: Традиційні платіжні системи на основі блокчейну, такі як Біткоїн, мають високу затримку транзакцій. Оскільки час підтвердження блоку в середньому становить близько 10 хвилин, а потенційно може бути набагато довшим, ця затримка робить ці системи непридатними для транзакцій в режимі реального часу, що перешкоджає їх використанню в повсякденній комерційній діяльності.
2. **Масштабованість**: Зі збільшенням кількості транзакцій мережа блокчейн може стати перевантаженою, що призводить до повільного виконання транзакцій і високих комісій за них. Масштабованість є значною проблемою для сучасних технологій блокчейн і нерозривно пов'язана з затримкою транзакцій.
3. **Ризики централізації**: В ідеалі, мережі блокчейн є децентралізованими і демократичними. Однак механізм консенсусу, який використовується в багатьох системах блокчейн, ненавмисно призвів до централізації, коли кілька потужних майнінг-пулів контролюють значну частину майнінгових потужностей мережі.
4. **Споживання енергії**: Майнінг, особливо в системах підтвердження роботи, вимагає значних обчислювальних ресурсів, що призводить до значного споживання енергії. Такий вплив на навколишнє середовище викликає занепокоєння щодо стійкості цих систем.
5. **Високі комісійні витрати**: Коли мережа стає перевантаженою, користувачі повинні платити вищу плату за пріоритетність своїх транзакцій. Це питання особливо актуальне для Ethereum, де високі тарифи на газ стали помітною проблемою.

Проект, з його новим підходом до архітектури блокчейну і механізму консенсусу, вирішує ці проблеми, прагнучи забезпечити масштабовану, ефективну і дійсно децентралізовану платіжну систему на основі блокчейну".

Зверніть увагу, що цей проект базується на загальних проблемах, виявлених в системах блокчейн, і може потребувати коригування, щоб ідеально відповідати специфіці вашого проекту.

## **3.2 Парадокс Пуассона та PoW**

У сфері блокчейну механіка алгоритму консенсусу Proof-of-Work (PoW), особливо в поєднанні з блоком, змодельованим як пуассонівський процес, призводить до інтригуючого парадоксу. Це те, що ми називаємо парадоксом Пуассона, який є чудовим явищем, що додає складнощів роботі в системі блокчейн.

Щоб проаналізувати цей парадокс, нам потрібно викласти специфіку нашої моделі. Блок моделюється як пуассонівський процес зі швидкістю λ. Це означає, що генерація блоків відбувається за пуассонівським розподілом із середнім часом між блоками, позначеним як 1/λ, що визначається бажаним рівнем складності операції майнінгу PoW. У випадку Біткоїна це приблизно 10 хвилин.

Пуассонівський процес характеризується випадковими подіями, які слідують експоненціальному розподілу, з інтервалами між подіями, які є статистично ідентичними і незалежними одна від одної. Ми моделюємо процес майнінгу як пуассонівський процес, фокусуючись виключно на моментах створення дійсних нових блоків.

Процес майнінгу в блокчейні PoW можна порівняти з азартною грою. Кожна спроба майнінгу схожа на підкидання монети, з дуже малим шансом на успіх. Ці спроби незалежні одна від одної і статистично ідентичні, що створює пуассонівський процес.

Наша модель робить кілька припущень. Ми припускаємо, що загальна кількість майнерів і їх колективна обчислювальна потужність є відносно постійною протягом певного періоду часу. Кожна машина майнера постійно намагається знайти правильні хеші - це єдині обчислення, які вона виконує. Таким чином, загальна кількість хешів, обчислених за одиницю часу, є постійною. У цій моделі ми припускаємо, що щосекунди обчислюється мільярд хешів.

Ми також враховуємо високий рівень складності хеш-пазла блоку-кандидата. Наприклад, якщо перші тридцять п'ять бітів хешу повинні бути нульовими для того, щоб блок був дійсним, ймовірність того, що конкретний nonce буде відповідати цьому критерію, становить 2^-35 або приблизно 3 × 10^-11. Отже, ймовірність того, що будь-який майнер розгадає хеш-пазл за задану секунду, дорівнює 0,03 - відносно невелике число.

Ця модель справедлива незалежно від кількості майнерів, їх індивідуальних обчислювальних потужностей, а також від того, чи працюють різні майнери над одними і тими ж блоками, чи над різними. Коли загальна обчислювальна потужність змінюється, припущення про фіксовану швидкість майнінгу може не спрацювати. Однак, загальна обчислювальна потужність не змінюється стрибкоподібно. Тому протягом короткого проміжку часу швидкість приблизно постійна.

Незважаючи на те, що більшість блоків видобувається протягом 10 хвилин, випадковий характер процесу означає, що завжди будуть певні блоки, на видобуток яких майнери витрачають більше або менше часу. Це призводить до того, що середній час підтвердження транзакції коливається в межах 10 хвилин.

Парадокс полягає в тому, що, незважаючи на те, що середній час підтвердження становить близько 10 хвилин, більшість людей чекають довше. Вибірковий аналіз блоків Біткоїна показує, що 60% блоків видобуваються довше, ніж за 10 хвилин, тоді як лише 40% видобуваються менш ніж за 10 хвилин. Цей перекіс у бік більшого часу підтвердження пояснюється довгим хвостом розподілу Пуассона, що призводить до того, що ми називаємо парадоксом Пуассона.

На час підтвердження біткоїн-транзакцій можуть впливати ще кілька факторів, але вони не мають прямого відношення до парадоксу Пуассона. Вони включають час, необхідний для отримання і хешування транзакцій з пулу пам'яті в заголовку блоку, а також час затримки, якщо комісія, пов'язана з транзакціями, занадто низька.

Таке розуміння парадоксу Пуассона в контексті PoW допомагає зрозуміти тонкощі функціонування блокчейн-систем і сприяє подальшій розробці запропонованого нами рішення.

У процесі нашого дослідження ми розробили набір моделей, спрямованих на розуміння нюансів епох майнінгу блоків у блокчейні Біткоїн. Наше дослідження включало симуляції та обширні дані, зібрані з блокчейну, але важливо визнати наявність певних проблем, включаючи глобально невідому швидкість хешування, яка диктує швидкість виявлення блоків, та історичну, але випадкову величину складності майнінгу.

Крім того, хоча дані про час прибуття блоків є стійкими, їх не можна вважати повністю надійними. Ми ввели модель точкового процесу, де процес надходження блоків імітує неоднорідний пуассонівський процес між періодами зміни складності. Швидкість пропорційна відношенню швидкості хешування до складності, але залишається незалежною від зміни складності. Дискретизуючи процес, ми можемо точно визначити момент зміни складності, а отже, і зміну швидкості надходження блоків, якщо припустити глобальну швидкість хешування.

Проте, оскільки глобальна швидкість хешування залишається високою, механізм регулювання складності демонструє значну затримку, що призводить до приблизної швидкості надходження блоків, яка на 11,5% перевищує базову швидкість в шість блоків на годину. В результаті, пропускна здатність транзакцій і загальний дохід майнерів від винагород перевищують базові прогнози. Крім того, моменти зменшення винагороди за блок вдвічі і, зрештою, видобутку всіх біткоїнів, за прогнозами, відбудуться раніше, ніж це було б, якби блоки видобувалися зі швидкістю шість блоків на годину.

Окрім моделювання процесу надходження блоків, ми виявили зв'язок між частотою надходження блоків та експоненціальним зростанням швидкості хешування. Ми запропонували практичне наближення, яке описує поведінку межі, незалежно від початкових умов і збурень процесу надходження блоків. Це наближення було підтверджено за допомогою симуляцій та даних з блокчейну.

Наше дослідження також підтвердило існування парадоксу Пуассона в контексті часу підтвердження транзакцій. Оскільки розподіл має довгий правий хвіст, більшість користувачів стикаються з довшим, ніж середній, часом підтвердження блоків. У той же час, меншість користувачів користуються швидкими підтвердженнями транзакцій. Розуміння цієї динаміки покращує наше розуміння тонкощів роботи блокчейн-систем, що є безцінним для подальшого розвитку та оптимізації цих платформ.

# **4. Аналіз парадоксу Пуассона**

Під час роботи з технологією блокчейн і, зокрема, з Біткоїном, можна спостерігати цікаве явище. Враховуючи, що система Біткоїн розроблена таким чином, що новий блок створюється приблизно кожні 10 хвилин, було б логічно припустити, що середній час очікування на підтвердження блоку буде коливатися навколо цієї 10-хвилинної позначки. Однак, як свідчать користувачі, багато користувачів повідомляють, що час очікування часто перевищує цей середній 10-хвилинний показник.

## **4.1 Гіпотеза**

Парадокс, з яким ми тут стикаємося, зазвичай називають парадоксом Пуассона. Цей парадокс, що ґрунтується на властивостях розподілу Пуассона, як відомо, призводить до контрінтуїтивних результатів у різних ситуаціях, зокрема, коли йдеться про час очікування і швидкість обслуговування.

У випадку з біткоїном парадокс Пуассона можна виразити через наступну гіпотезу: *Незважаючи на те, що середній час підтвердження блоку встановлений на рівні приблизно 10 хвилин, більшість користувачів в кінцевому підсумку чекають на підтвердження блоку більше 10 хвилин*.

У цьому розділі звіту ми зануримося в цю гіпотезу глибше. Ми прагнемо математично описати цей парадокс, провести аналіз на основі даних блокчейну Біткоїна і пояснити реальні наслідки цього особливого явища в екосистемі блокчейну.

Наш аналіз сприятиме кращому розумінню динаміки блокчейн-систем і допоможе нам у розробці та впровадженні ефективних рішень на основі блокчейн-технологій. Вивчення цього парадоксу є не просто теоретичною вправою; він має глибокі наслідки для того, як користувачі взаємодіють з технологією блокчейн і як розробники проектують системи на основі блокчейну. Розуміння цього явища має вирішальне значення для покращення користувацького досвіду, зміцнення довіри та прийняття блокчейн-систем.

**4.2 Математична модель**

Намагаючись дослідити, чи надходження блоків слідує пуассонівському процесу, ми розуміємо, що глобальна швидкість хешування H(t), емпірично або параметрично змодельована, визначає швидкість хешування для кожного надходження блоків за допомогою вибіркового стохастичного процесу, позначеного як Xi(t).

Давайте розберемо цей сценарій на три ключові ситуації:

* **Ситуація 1**: Детерміноване коригування складності

У випадку детермінованого коригування складності, коригування виконується в детерміновані моменти часу, позначені через yn, які не збігаються зі стохастичними моментами надходження блоків. Отже, швидкість надходження блоків, λ(t), залишається нечутливою до надходжень блоків на попередньому відрізку. За відсутності затримки модель узгоджується з неоднорідним пуассонівським процесом в межах кожного сегмента.

* **Ситуація 2**: Адаптація до стохастичної складності

Коли ми переходимо до стохастичного коригування складності, складність коригується в довільні моменти часу, після кожного сегмента 2016 блоків, дотримуючись попередньо визначеного рівняння. У сценарії, позбавленому затримки поширення, кожен сегмент процесу має форму неоднорідного пуассонівського процесу зі швидкістю λ(t) = H(t)/Di. Враховуючи, що швидкість надходження блоків, λ(t), залежить від початкового і кінцевого надходження блоків в попередньому сегменті блокчейну, процес не відображає пуассонівський розподіл для послідовних часових періодів сегмента.

* **Ситуація 3**: Затримка поширення

При наявності затримки розповсюдження процес надходження блоків навіть не імітує неоднорідний пуассонівський процес в межах одного сегмента.

У наступному розділі ми більш детально розглянемо ці сценарії і висвітлимо складнощі та особливості процесу прибуття блоків в технології блокчейн. Порівняємо їх моделювання до даних про позначку часу з блокчейну біткоїна.

Отже, ми не будемо враховувати динамічну складність і змоделюємо сегмент з 2016 блоків, що дорівнює приблизно місяцю в реальному часі, або 20160 хвилин. Ми також припускаємо, що розподіл блоків у мережі відбувається миттєво, без затримок.

Точковий процес N є процесом Пуассона на , якщо він має наступні дві властивості.

1. Випадкова кількість точок N([a, b)) точкового процесу N, розташованих в обмеженому інтервалі [a, b) ⊂ R, є пуассонівською випадковою величиною із середнім Λ([a, b)), де Λ є невід’ємною мірою Радона.
2. Кількість точок точкового процесу N, розташованих на k інтервалах [a1, b1), . . . , [ak, bk) утворюють k незалежних пуассонівських випадкових величин із середніми Λ([a1, b1)), . . . ,Λ([ak, bk)).

Відтепер будемо записувати N([a, b)) як N(a, b) і Λ([a, b)) = Λ [a, b) для зручності. Перша властивість передбачає що

і , а друга властивість – це Основна причина придатності процесу точки Пуассона і зазвичай це основа статистичних тестів, які вимірюють адекватність моделей Пуассона. Розподіл Пуассона N(a, b) означає, що його дисперсія Var[N(a, b)] = Λ(a, b), факт який також використовується як статистичний тест. Міра Λ відома як міра інтенсивності або середнє значення міри процесу точки Пуассона. Припустимо, що a існує така функція λ(t), що

Тоді λ(t) визначена як функція швидкості. Якщо λ(t) є сталою λ > 0, то процес називається однорідним точковим процесом Пуассона. Інакше процес називають неоднорідним або **неоднорідним точковим процесом Пуассона**. Якщо обмежити нашу увагу інтервалом невід’ємних чисел [0, ∞), міра інтенсивності задається формулою

Для пуассонівського процесу N з мірою інтенсивності Λ ймовірність існування n точок в інтервалі [a, b) дорівнює

Час надходження та час між надходженнями: розглянемо точковий процес {X(i)}i≥1, визначений на невід’ємних дійсних числах із майже напевно кінцевою кількістю точок у будь-якому обмеженому інтервалі. Тоді ми можемо інтерпретувати точки процесу як часи добування нових блоків та розмістити їх у порядку зростання, X1 ≤ X2 ≤ . . .. Тоді відстані між сусідніми точками дорівнюють Ti := Xi − Xi−1 для i = 2, 3, . . . і T1 = X1. Випадкові величини Ti відомі як час очікування або час між надходженнями. Для однорідного процесу Пуассона зі швидкістю λ відповідні часи між надходженнями є незалежними та однаково розподіленими експоненціальними випадковими величинами із середнім значенням 1/λ

Де властивість експоненціального розподілу без пам’яті було використано. Це не стосується неоднорідного точкового процесу Пуассона з інтенсивністю λ(t), де перший час між надходженнями T1 = X1 має розподіл

За першого часу очікування T1 = t1 умовний розподіл другого часу очікування T2 є

і так далі для k ≥ 2

Можна показати, що k-й час надходження Xk має розподіл

З щільністю

Умова на n точок пуассонівського процесу, що існує в деякому обмеженому інтервалі [0, t]. Ми називаємо ці точки умовним часом надходження блоку. Якщо процес Пуассона є однорідним, то умовні часи надходження рівномірно і незалежно розподілені, утворюючи n рівномірних випадкових величин на [0, t]. Ця різниця між часом очікування Ti та умовним часом надходження Ui відіграє роль у тесті Пуассона.

Для неоднорідного пуассонівського процесу кожна точка Ui незалежно розподілена на інтервалі [0, t] із розподілом

,

Якщо розподіл кожного Ui відомий і оборотний, то кожен Ui може бути перетворений в рівномірну випадкову величину на [0, 1], що призводить до n незалежних рівномірних випадкових величин. Іншими словами, Λ(t) перетворює процес Пуассона на однорідний процес Пуассона з густиною один на відрізку дійсних чисел. Отже, статистичні методи для неоднорідних процесів Пуассона часто передбачають перетворення даних перед виконанням аналізу.