Міністерство Освіти і Науки України
Київський Національний Університет Імені Тараса Шевченка
Факультет Інформаційних Технологій

Вузол електронної системи безготівкових розрахунків

виконав
студент гр. ІПЗ-43 Гоша Давід Олександрович
науковий керівник
д.т.н. с.н.с. Порєв Геннадій Володимирович

АКТУАЛЬНІСТЬ

Технологія блокчейн стрімко розвивається і знаходить все більше застосувань у різних сферах. Однією з найперспективніших областей її використання є платіжні системи, де блокчейн має потенціал здійснити революційні зміни. Однак існуючі моделі платіжних систем, засновані на блокчейні, стикаються з рядом обмежень і проблем, які заважають їх широкому впровадженню та використанню. Цей проект присвячений вирішенню цих проблем, щоб прокласти шлях до більш ефективної та надійної платіжної системи на основі блокчейну. Аналізуючи сучасні виклики та пропонуючи інноваційні рішення, ми прагнемо сприяти розвитку платіжних систем, які зможуть забезпечити швидкі, безпечні та прозорі транзакції в глобальному масштабі.

МЕТА

Мета роботи - вдосконалення існуючих блокчейн-систем шляхом:

01
Зменшення затримки транзакцій.

02
Мінімізації споживання енергії.

03
Зниження ризиків централізації.

04
Зменшення високих комісій за транзакції.

Для досягнення поставленої мети планується розробка масштабованої та ефективної блокчейн-системи, яка дозволить вирішити вищезазначені проблеми та підвищити ефективність роботи блокчейну. Особлива увага приділяється створенню екологічно чистої та демократичної блокчейн-мережі, яка працює в режимі реального часу і підходить для повсякденної комерційної діяльності. Ця система повинна бути не лише технологічно досконалою, але й доступною та надійною для широкого кола користувачів, сприяючи тим самим її масовому впровадженню та використанню.

ЗАДАЧІ РОБОТИ

ГІБРИДНА МЕРЕЖА

Розробка блокчейн-системи з гібридною архітектурою для зменшення затримки транзакцій та підвищення масштабованості мережі.

ГІБРИДНИЙ КОНСЕНСУС

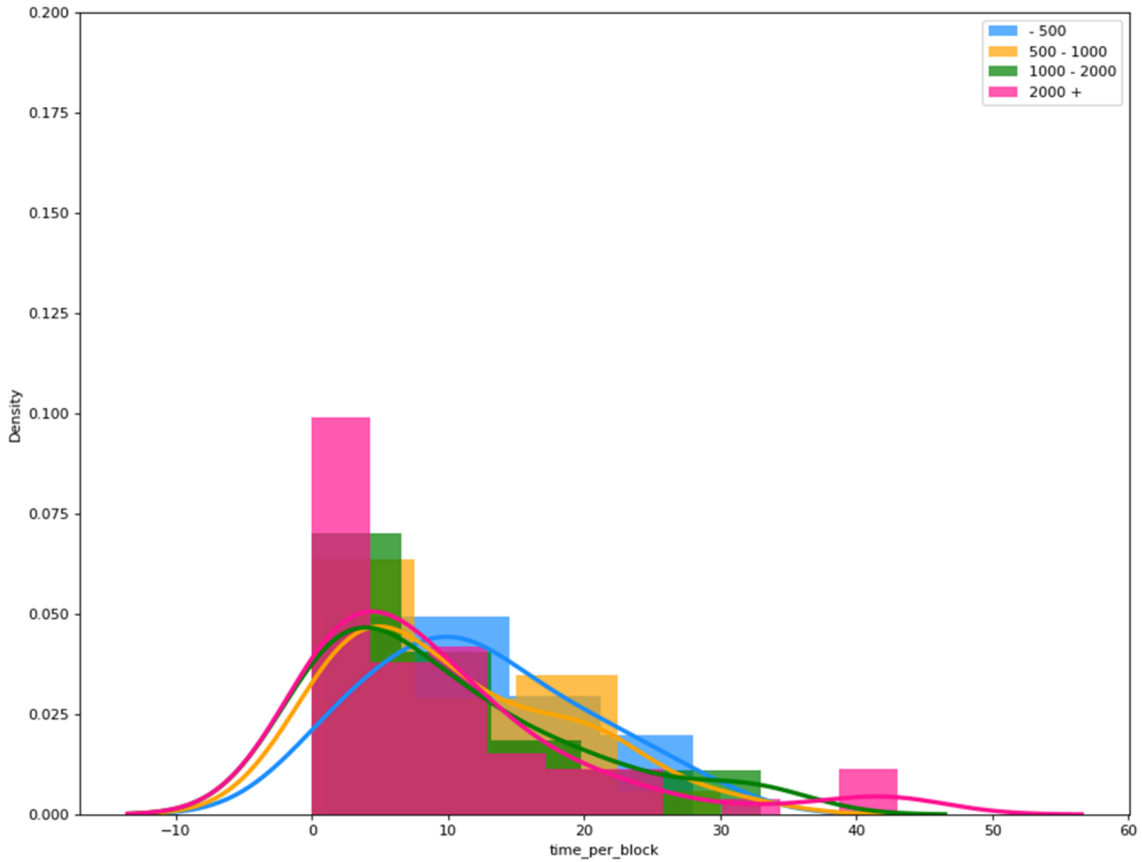
Реалізація гібридного механізму консенсусу (PoET + PoW) для зменшення ризиків централізації та зниження енергоспоживання.

ЗНИЖЕННЯ КОМІСІЙ

Вирішення проблем високих комісій шляхом підтримки ефективної роботи мережі при великих обсягах транзакцій.

АНАЛІЗ ПАРАДОКСУ ПУАССОНА

Доказ парадоксу Пуассона криється в початковій гістограмі, особливо в її довгому правому хвості. Хоча середній час очікування підтвердження становить 9,9 хвилин, більшість респондентів чекають понад 10 хвилин. Це пояснюється більшою ймовірністю виявлення блоку в інтервалі 10-40 хвилин порівняно з інтервалом 0-10 хвилин через розподіл Пуассона.



МЕТОДИКА ДОСЛІДЖЕННЯ

Аналіз Парадоксу Пуассона:

Огляд існуючих блокчейн-систем. Визначення їх переваг та недоліків.

Розробка Гібридної Системи:

Створення моделі гібридної блокчейн-архітектури. Тестування її ефективності.

Аналіз Поточного Стану:

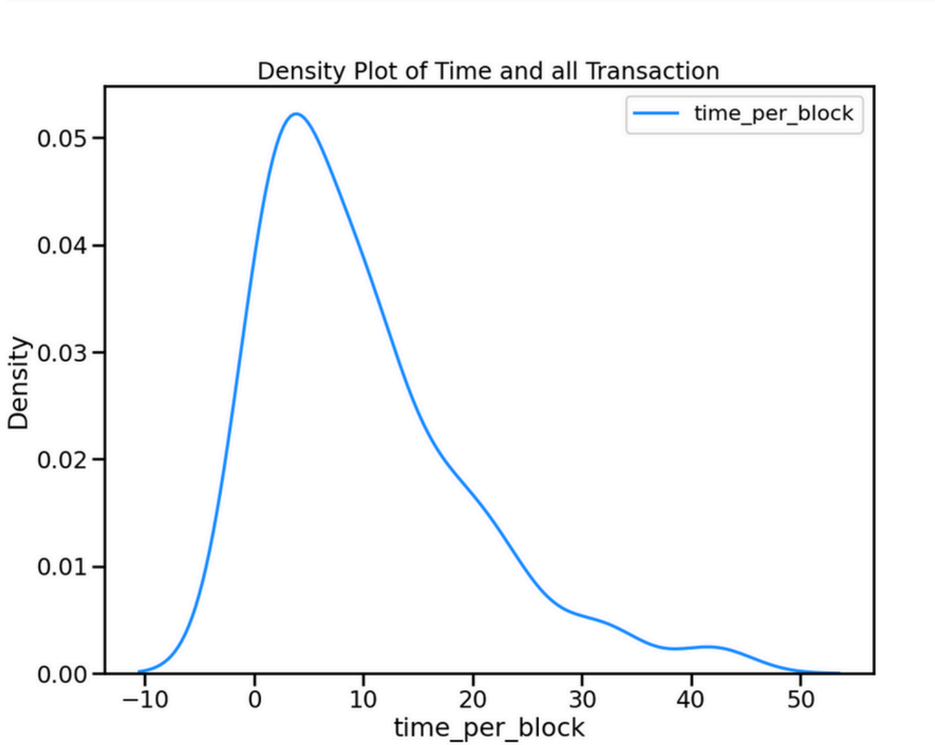
Дослідження розподілу часу підтвердження транзакцій. Використання гістограм та статистичних методів.

Мета Аналізу

Аналіз парадоксу Пуассона дозволяє виявити приховані закономірності та оптимізувати алгоритми підтвердження транзакцій для підвищення загальної ефективності системи.

ПРОБЛЕМА ЧАСУ ОЧІКУВАННЯ

Час підтвердження блоку	Відсоток вибірки
0 – 10 хвилин	40 %
10 – 40 хвилин	60 %



Таким чином, 2/5 нашої вибірки отримали підтвердження транзакції менш ніж за 10 хвилин, тоді як решта 3/5 були свідками того, що час підтвердження перевищував 10 хвилин. Це те, що ми називаємо парадоксом Пуассона.

МЕРЕЖЕВА АРХІТЕКТУРА БЛОКЧЕЙНУ

1. Гібридна мережа

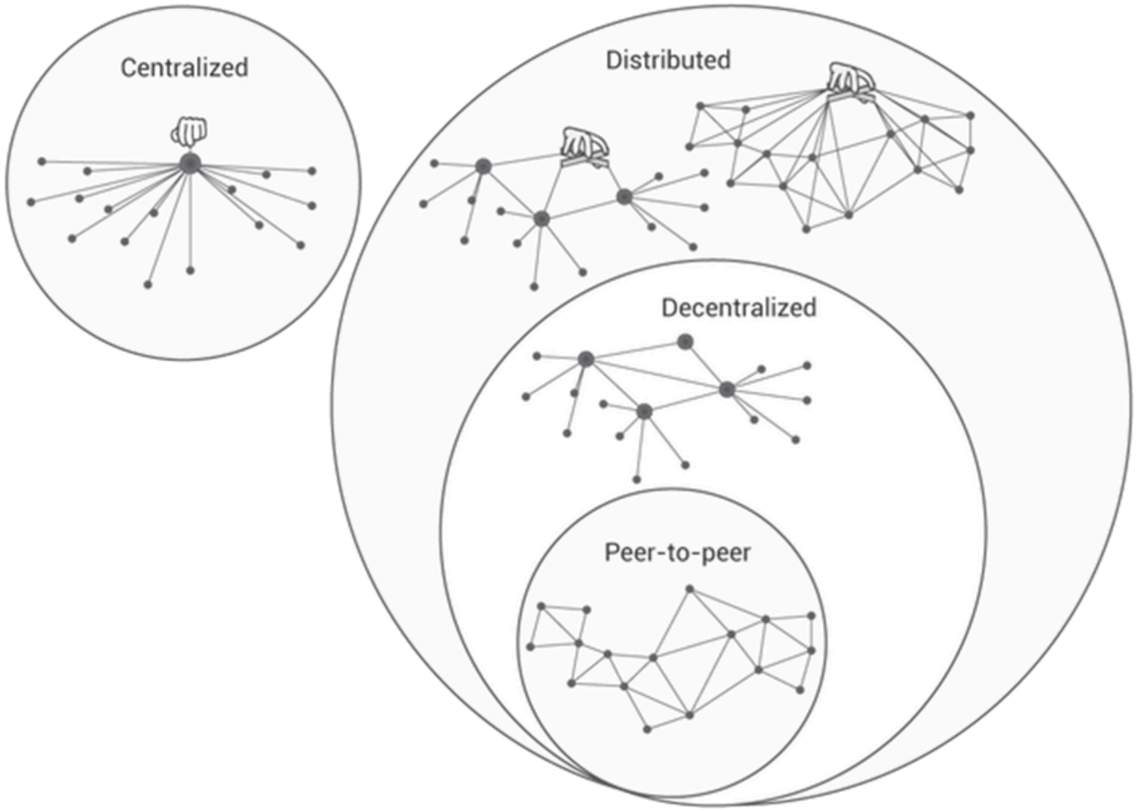
Цей блокчейн-додаток використовує гібридну мережеву архітектуру, яка поєднує клієнт-серверні та однорангові характеристики. Це забезпечує ефективну комунікацію між клієнтами, вузлами, серверами пулу та серверами часу.

2. Надійність мережі

Мережевий потік ретельно планується для забезпечення максимальної безпеки і зручності для широкого кола користувачів. Гібридна архітектура дозволяє мережі зберігати надійність навіть при DDoS-атаках.

3. Захист від атак

Напади на сервери можуть погіршити продуктивність мережі, але не порушують її загальну роботу завдяки гібридній архітектурі.



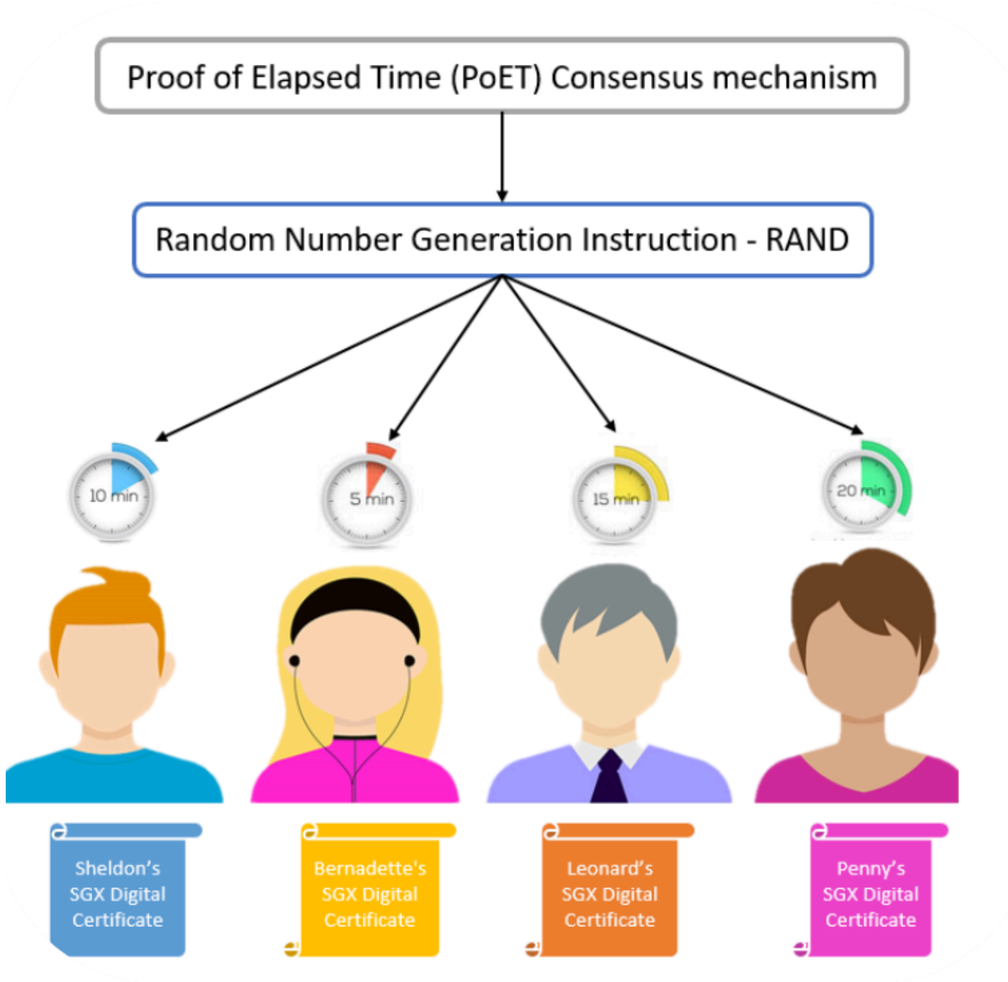
МЕХАНІЗМ КОНСЕНСУСУ В ЗАСТОСУНКУ

Механізм консенсусу, що використовується в додатку, це гібридна модель, яка поєднує в собі Доказ часу, що минув (Proof of Elapsed Time, PoET) і Доказ роботи (Proof of Work, PoW).

Ця гібридна модель забезпечує:

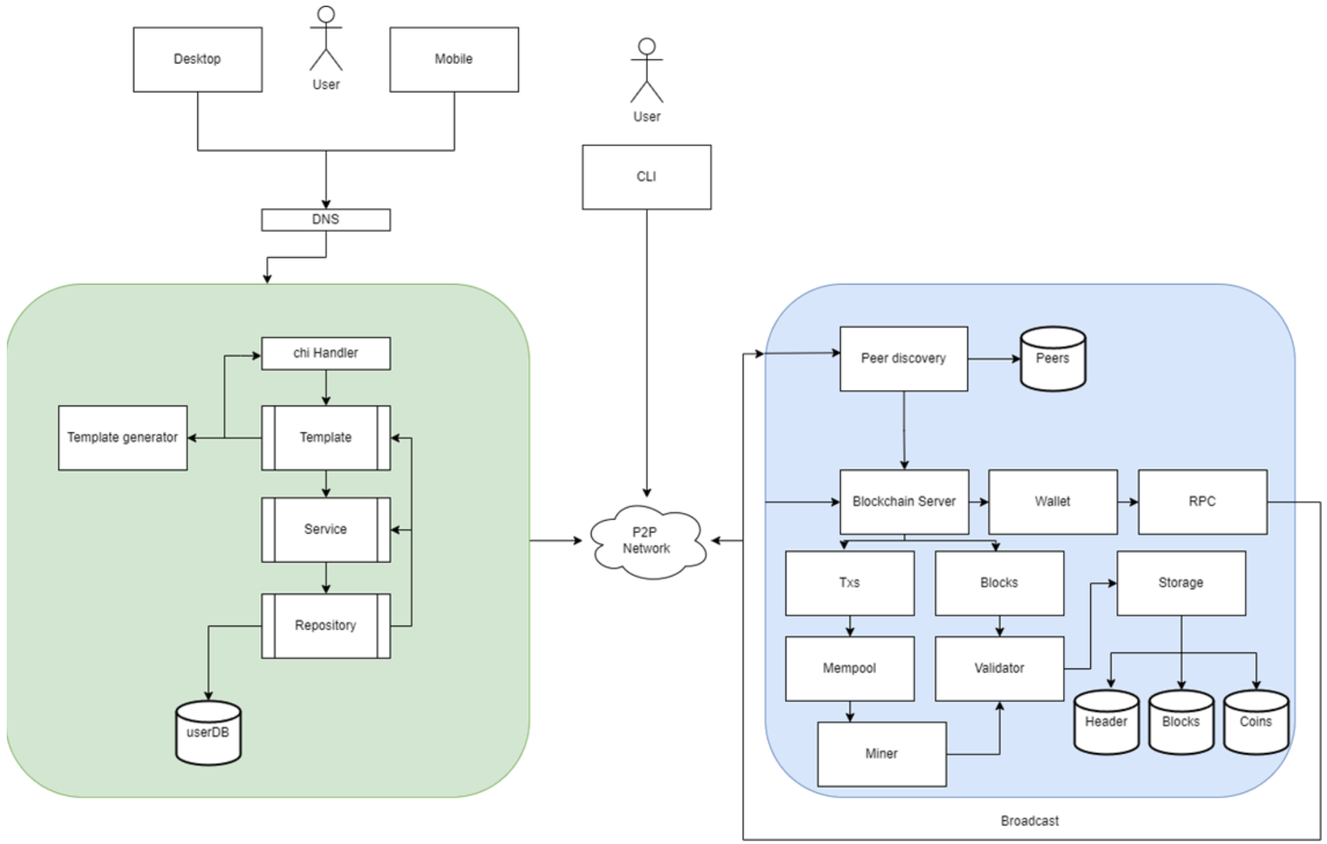
- **Справедливість**: Кожен вузол-учасник має рівні шанси на видобуток блоку, що підтримує децентралізацію.
- **Безпеку**: Поєднання двох механізмів гарантує захист системи навіть при уразливості одного з них.

Структура і компоненти блокчейн-додатку забезпечують надійну, децентралізовану систему, гарантуючи безпеку і цілісність транзакцій. Це робить його придатним для різноманітних застосувань, включаючи криптовалюти та децентралізовані додатки (dApps).

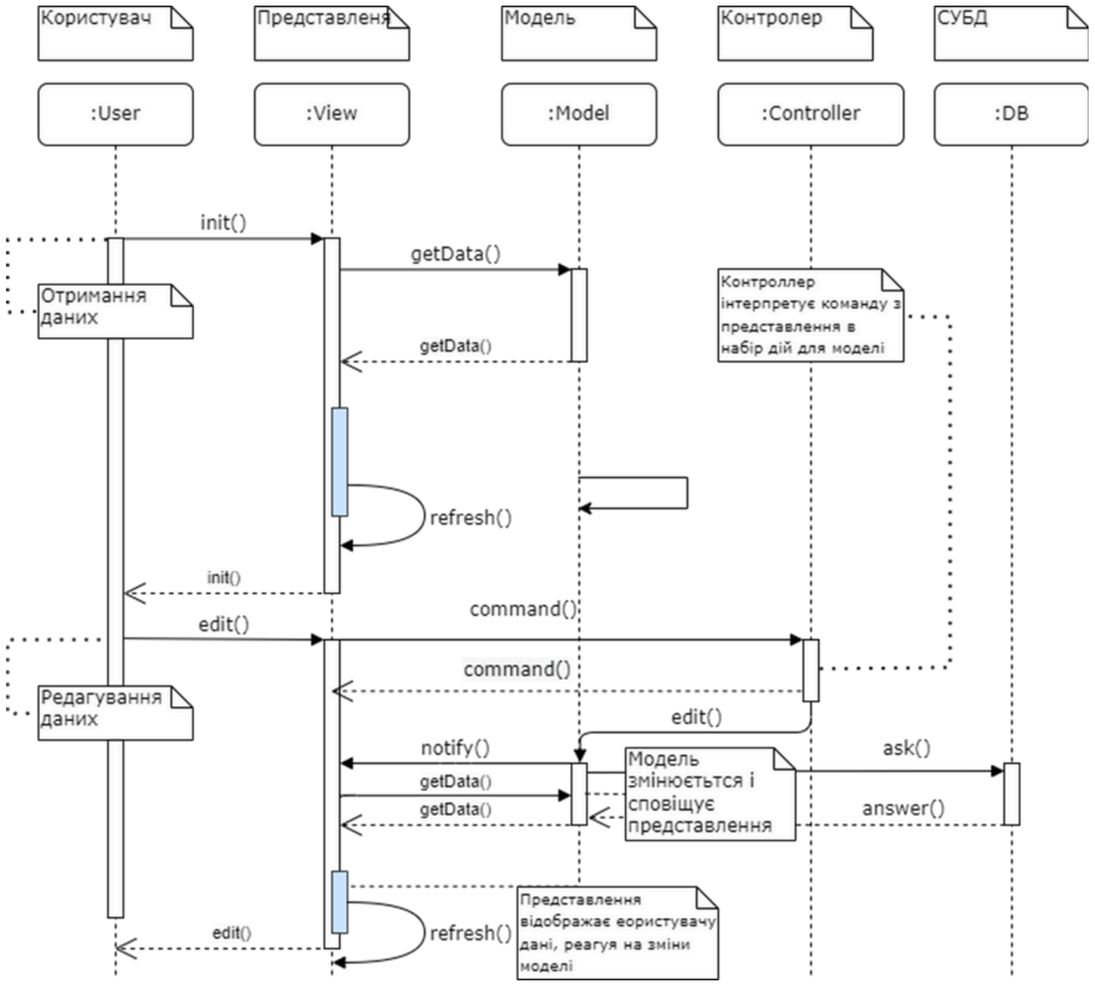


АРХІТЕКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Архітектура системи електронних платежів на основі блокчейну забезпечує безпеку та зручність. Вона включає веб-гаманець, консольний інтерфейс, вузли блокчейну для зберігання реєстру та перевірки транзакцій, децентралізований реєстр усіх транзакцій та mempool для тимчасового зберігання непідтверджених транзакцій. Процес перевірки гарантує включення до блокчейну тільки дійсних транзакцій. Усі компоненти працюють разом для забезпечення надійності.



UML ДІАГРАМА КОМПОНЕНТІВ



АРХІТЕКТУРА MVC

Web-гаманець використовує архітектуру MVC для оптимізації операцій та покращення користувацького досвіду. Користувач взаємодіє з інтерфейсом через Представлення, яке оновлюється Контролером на основі змін у Моделі, що обробляє дані з СУБД. Такий підхід підвищує продуктивність та ефективність системи.

ВИСНОВКИ

Зменшення затримки транзакцій

Час підтвердження знизився до 10 секунд, що збільшило пропускну здатність до 6000 TPS порівняно з 7 TPS у біткоїна. Середня комісія за транзакцію знизилася до $0.0008 в перерахунку, роблячи систему більш економічно вигідною для користувачів.

Зниження ризиків централізації:

Відсутність потреби у великих майнінг-пулах сприяє більш рівномірному розподілу потужностей серед вузлів, зменшуючи ризики централізації та підвищуючи рівень децентралізації мережі.

Мінімізація споживання енергії:

Впровадження PoET дозволяє майнінг на звичайному CPU, що знижує споживання енергії на 99.95% порівняно з PoW, який споживає близько 200 ТВт·год на рік, що еквівалентно споживанню енергії невеликою країною.

Зменшення високих комісій за транзакції:

Висока пропускна здатність знизила середні комісії у ~851 раз, роблячи систему більш економічно вигідною.

Публікації Гоша. Д. " Розробка протоколу консенсусу для блокчейн-платформи на основі делегованого доказу частки володіння та багатопідписів". 11-тій Східно Європейській конференції Математичні та програмні технології Internet of Everything, 11-12.04.2024. с. 99 – 100