Слайд 1 **Вступ**: Технологія блокчейн стрімко розвивається та знаходить все більше застосувань, зокрема в платіжних системах. Вона має потенціал здійснити революційні зміни, забезпечуючи швидкі та прозорі транзакції в глобальному масштабі. Однак існуючі моделі мають певні обмеження, які заважають їх широкому впровадженню. Ця робота спрямована на вирішення цих проблем для створення ефективної та надійної платіжної системи на основі блокчейну.

Слайд 2 **Мета та завдання дослідження**:

* Мета роботи - вдосконалити існуючі блокчейн-системи шляхом зменшення затримки транзакцій, мінімізації споживання енергії, зниження ризиків централізації та зменшення високих комісій.
* Заплановано розробити масштабовану та ефективну блокчейн-систему, яка дозволить вирішити ці проблеми та підвищити ефективність роботи блокчейну.

Слайд 3 **Основні задачі дослідження**:

Для досягнення мети було поставлено кілька важливих задач. По-перше

1. Розробка гібридної архітектури для зменшення затримки транзакцій.
2. Реалізація гібридного механізму консенсусу, який поєднує доказ часу (PoET) і доказ роботи (PoW), що дозволяє знизити енергоспоживання та ризики централізації.
3. Розгляд зниження комісій за рахунок ефективної роботи мережі.

Слайд 4 **Аналіз аналогічних систем**: Дослідження показало, що середній час очікування підтвердження транзакції в аналогічних системах становить 9,9 хвилин. Проте більшість користувачів змушені чекати більше 10 хвилин через нерівномірний розподіл часу підтвердження транзакцій, що відоме як парадокс Пуассона.

Слайд 5 **Методологія дослідження**:

1. Вступ: Визначення мети дослідження - підвищення ефективності блокчейн-системи.
2. **Аналіз поточного стану**: Аналіз існуючих блокчейн-систем для визначення їхніх переваг і недоліків, що допомагає зрозуміти, які аспекти потребують вдосконалення.
3. **Розробка гібридної системи**: Створення моделі гібридної блокчейн-архітектури, що поєднує PoET і PoW. Тестування системи для оцінки її ефективності у зменшенні затримок транзакцій та енергоспоживання.
4. **Аналіз парадоксу Пуассона**: Дослідження розподілу часу підтвердження транзакцій з використанням гістограм та статистичних методів. Виявлення, що більшість транзакцій підтверджуються за час, більший за середній, через розподіл Пуассона.
5. **Мета аналізу**: Виявлення прихованих закономірностей у затримках транзакцій для оптимізації алгоритмів підтвердження та підвищення загальної ефективності блокчейн-системи.

Слайд 6 **Аналіз парадоксу Пуассона**: З'ясовано, що 40% транзакцій підтверджуються менш ніж за 10 хвилин, тоді як 60% – за 10-40 хвилин. Це явище, відоме як парадокс Пуассона, вказує на необхідність покращення механізмів для прискорення процесу підтвердження транзакцій.

Слайд 7 **Запропонована архітектура системи**: У проекті реалізована гібридна мережа, яка поєднує клієнт-серверну та однорангову моделі. Це дозволяє забезпечити ефективну комунікацію між усіма учасниками мережі. Завдяки такій архітектурі система залишається стабільною і надійною, навіть під час атак на мережу.

Слайд 8 **Гібридний механізм консенсусу**: У системі використовується гібридний механізм консенсусу, який поєднує PoET і PoW. Це дозволяє забезпечити справедливість і безпеку системи. Кожен вузол має рівні шанси на видобуток блоку, що підтримує децентралізацію. Навіть якщо один механізм стає вразливим, інший забезпечує захист системи.

Слайд 9 **Компоненти системи**: Система складається з кількох ключових компонентів:

* Веб-гаманець для користувачів
* Консольний інтерфейс для розробників
* Вузли блокчейну для зберігання та перевірки транзакцій Всі ці компоненти працюють разом, забезпечуючи безпечне та зручне управління транзакціями. Кожна транзакція ретельно перевіряється перед включенням до блокчейну.

Слайд 10 **Архітектура MVC (Model-View-Controller)**:

* **Модель** керує даними і бізнес-логікою, обробляючи та зберігаючи інформацію в базі даних.
* **Представлення** відповідає за відображення даних користувачу і оновлюється при зміні даних у моделі.
* **Контролер** обробляє команди користувача, передає їх моделі і оновлює представлення.

Наприклад, при створенні нової транзакції користувачем, контролер обробляє цю команду, модель зберігає дані, а представлення оновлюється, щоб показати нову транзакцію. Використання MVC робить додаток більш структурованим і зручним для підтримки та розвитку.

Слайд 11 **Висновки та результати**:

* **Гібридний консенсус PoW/PoET** значно підвищує ефективність блокчейн-системи, знижуючи затримки, енергоспоживання та ризики централізації.
* **Оптимізована архітектура мережі** забезпечує високу масштабованість та баланс між децентралізацією та продуктивністю.
* **Аналіз парадоксу Пуассона** в PoW дозволив розробити рішення для зменшення часу підтвердження транзакцій.
* Впроваджено **механізми захисту від атак Sybil та безпеки в Довіреному Середовищі Виконання (ТЕЕ)**, підвищуючи стійкість та надійність системи.
* **Практична реалізація**, включаючи веб-гаманець та CLI, підтверджує ефективність запропонованого рішення в порівнянні з існуючими системами.
* Дослідження пропонує **інноваційні підходи** для створення більш ефективних, безпечних та зручних децентралізованих платіжних систем на основі блокчейну.