ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

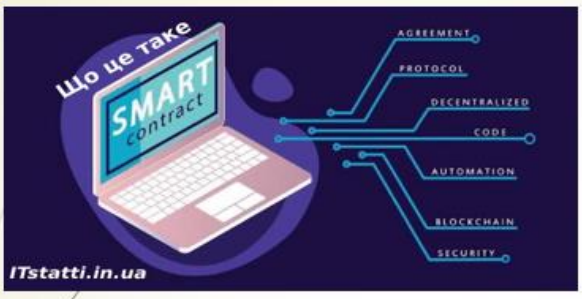
МЕТОД БАЛАНСУВАННЯ ДЛЯ КЕРУВАННЯ ДАНИМИ НА БАЗІ СМАРТ-КОНТРАКТІВ

Виконав: студент групи СПм-23-4
Шаповал Антон Сергійович
Керівник : зав. кафедри ЕОМ
Коваленко Андрій Анатолійович

2025

2

СМАРТ-КОНТРАКТИ



Смарт-контракти — це програми, що працюють у блокчейні. Вони автоматизують виконання умов між сторонами. Смарт-контракти не потребують посередників або третіх сторін. Це підвищує довіру і знижує витрати.

Рік появи поняття – 1994. Ідея - замінити юридичні договори кодом Смарт-контракт — це код, який зберігається в блокчейні. Він запускається, коли виконуються певні умови. Після запуску його вже не змінити.

Головні переваги смарт-контрактів:

– смарт-контракти зменшують людський фактор;
– автоматизація знижує ризик помилок;
– процеси відбуваються швидше і дешевше, не потрібні юристи;
– вони підвищують прозорість. усі дії видно в блокчейні;
– дані не можна видалити або змінити, це створює довіру між сторонами;
– контракти працюють цілодобово: це корисно для міжнародних операцій.

3

БЛОКЧЕЙН МЕРЕЖА

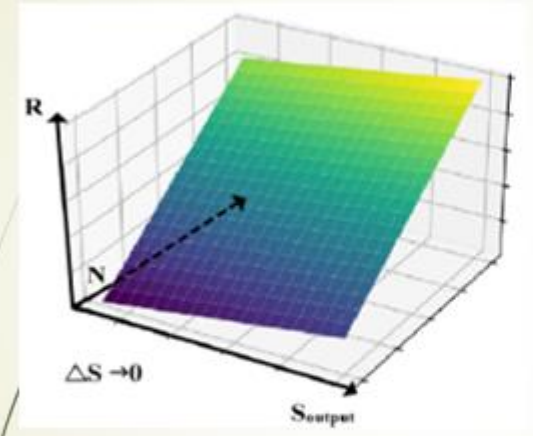
- Блокчейн мережа - це децентралізована база даних, яка складається з ланцюжка блоків, де кожен блок містить інформацію про транзакції або інші дані.
- Ці блоки пов'язані між собою криптографічно, утворюючи незмінний та прозорий реєстр.

Блокчейн мережа - це революційна технологія, яка забезпечує безпечне, прозоре та надійне зберігання і обмін даними:

Децентралізована: не має центрального органу управління, а її дані зберігаються на багатьох комп'ютерах (вузлах) одночасно.
Незмінна: після додавання блоку в ланцюжок, його неможливо змінити або видалити без згоди більшості вузлів мережі.
Прозора: зазвичай, всі транзакції в блокчейн-мережі є відкритими для перегляду.
Криптографічно захищена: кожен блок містить інформацію про попередній блок, створюючи нерозривний ланцюжок, захищений криптографічними методами.
Розподілена: дані блокчейну розподілені між багатьма учасниками мережі, що робить її стійкою до збоїв та маніпуляцій.
Використання: використовується для різних цілей, включаючи криптовалюти (наприклад, Bitcoin), управління ланцюгами поставок, голосування тощо.

4

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ



R – надійність
N – кількість вузлів
S_{output} – розмір даних в системі
ΔS – показник балансу розподілу даних

Зі збільшенням кількості вузлів має збільшуватись вільний простір, доступний для зберігання нових файлів, а також має підвищуватись надійність системи

Централізовані сервери використовуються багатьма організаціями, оскільки вони дешеві та прості у розгортанні. Однак централізовані сервери мають одну або кілька єдиних точок відмови та не підтримують масштабованість. Крім того, сервери резервного копіювання не вирішують проблему масштабованості, яка вважається вимогою для організацій, де потрібно зберігати величезну кількість файлів.

5

МЕТА ТА ЗАВДАННЯ РОБОТИ

Мета дослідження - підвищення продуктивності децентралізованих інформаційних систем на базі смарт-контрактів за рахунок удосконалення методу балансування для керування даними.

Основні задачі дослідження:

1) визначити підходи до розподілу даних в децентралізованих системах;
2) визначити підходи до контролю доступу в децентралізованих системах зберігання даних;
3) удосконалити метод балансування для керування даними на базі смарт-контрактів та провести оцінку його ефективності.

6

ПОСТАНОВКА ЗАВДАННЯ

$$S_{Output} = S_{Input} + SR_{educancy} + SM_{etadata} + S_{AccessControl}. \quad (1)$$

$$S_{Metadata} + S_{AccessControl} \ll S_{Input} \quad (2)$$

$$S_{Output} \approx S_{Input} + S_{Reducancy}. \quad (3)$$

$$DistrSystem <S_{Output}, \Delta S, R, \boldsymbol{N}> \quad (4)$$

$$max_R min_{SOutput,\ \Delta S} (DistrSystem < S_{Output}, \Delta S, R, \boldsymbol{N}>). \quad (5)$$

При роботі зі смарт-контрактами існує кілька обмежень:

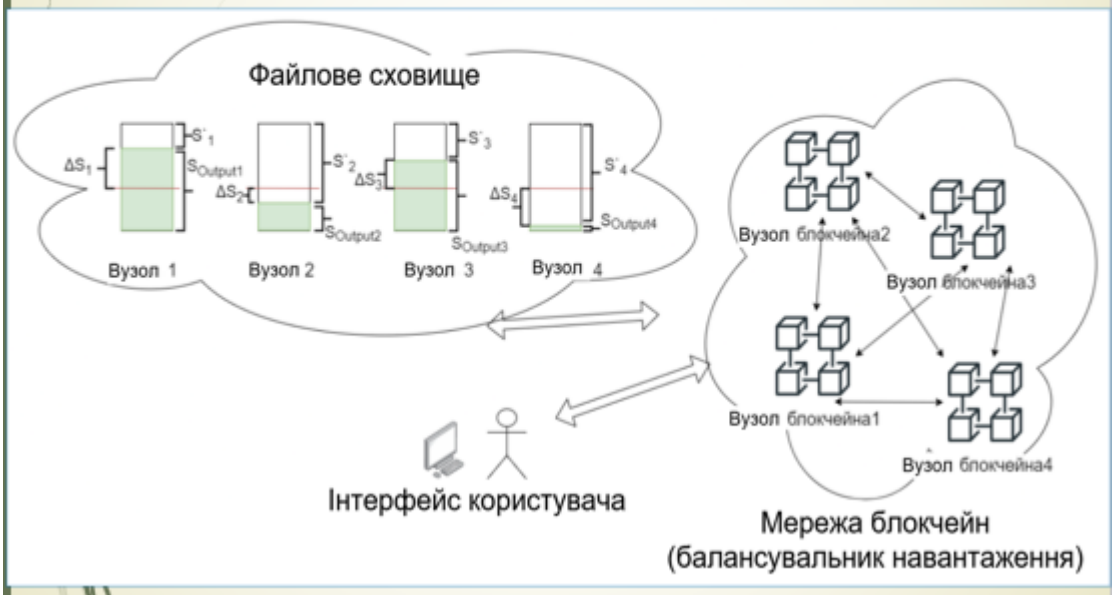
1. **Обмеження мови програмування**: не всі мови програмування підтримуються в мережі блокчейн.

2. **Складні типи даних і структури не підтримуються**, що обмежує можливості роботи із змінними.

3. **Обмежені бібліотеки і функціональність**: смарт-контракти мають обмежені бібліотеки і функціональність у порівнянні з програмуванням спільного призначення.

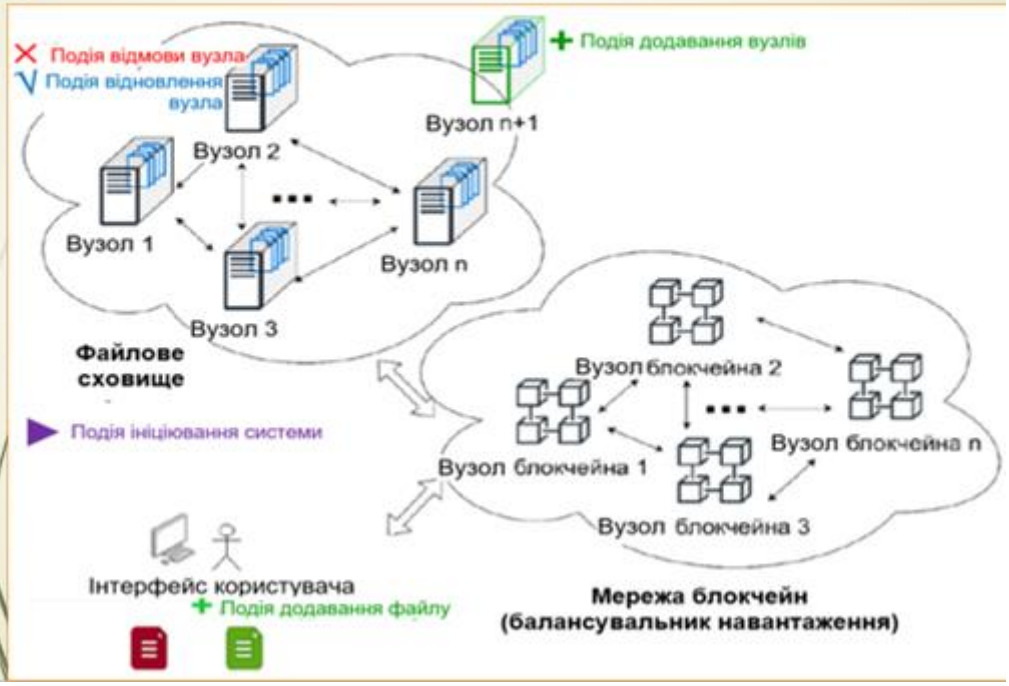
7

ПРОПОНУЄМА АРХІТЕКТУРА ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ



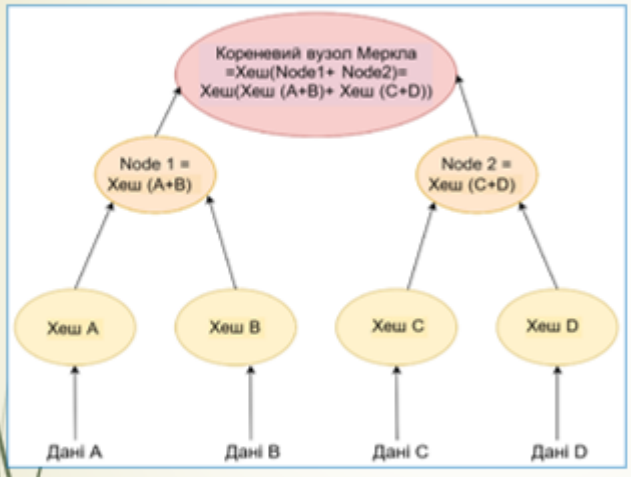
8

ПОДІЇ, ЩО ВПЛИВАЮТЬ НА РОЗПОДІЛ ДАНИХ



9

ДЕРЕВО МЕРКЛА



Дерево Меркла, також відоме як дерево хешів, - це структура даних, яка використовується для ефективної перевірки цілісності великих обсягів даних. Воно є бінарним деревом, в якому кожна листяна вершина містить хеш від блоку даних, а кожна внутрішня вершина містить хеш від об'єднання хешів її дочірніх вершин. Корнева вершина містить хеш від усього набору даних.

Основні характеристики дерева Меркла:

- **Швидка перевірка цілісності:** дозволяє швидко перевірити, чи були змінені будь-які дані в наборі.
- **Ефективне зберігання:** завдяки використанню хешів, дерево Меркла дозволяє зберігати великі обсяги даних компактно.

10

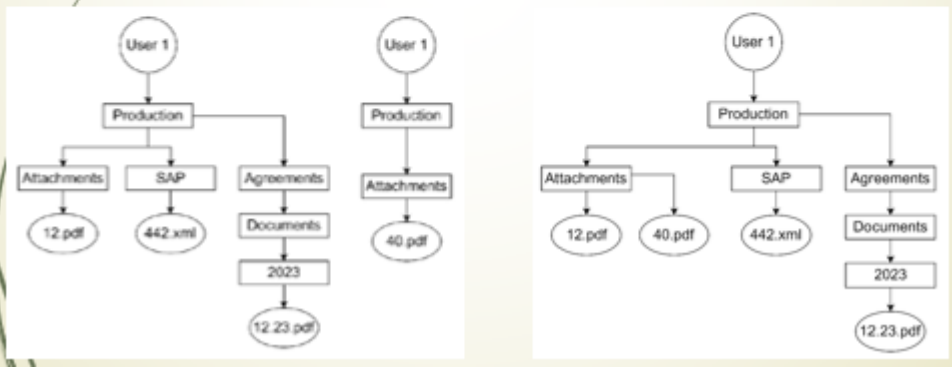
ФОРМУВАННЯ ДЕРЕВА МЕРКЛА

Етап 1. У кожному віртуальному диск, вибраному блокчейном, створюється дерево для кожного користувача.

Етап 2. Кожен вузол об'єднує ці дерева в одне дерево, яке показує, до яких файлів користувач має доступ в цьому вузлі.

Етап 3. Після цього дерево стискається шляхом об'єднання вузлів дерева, що мають один дочірній елемент, в один вузол, щоб мінімізувати розмір дерево.

Етап 4. Отримане дерево перетворюється в двійкове дерево, щоб мінімізувати розмір доказу Меркла.




11
АРХІТЕКТУРА DECSTORE
З МОДЕЛЛЮ КОНТРОЛЮ ДОСТУПУ
VD6-EC
VD4-P1
VD3-P1
VD1-P1
VD6-P1
VD5-P2
VD4-EC
VD2-P1
VD5-P1
VD3-EC
VD1-P2
VD6-P2
VD4-P2
VD2-EC
VD1-EC
VD5-EC
VD3-P2
VD2-P2
Роль 1
Роль 3
Роль 5
Роль 1
Роль 4
Роль 2
Роль 3
Роль 4
Роль 2
Роль 5
Компоненти сховища дозволів
Ролі
Вузол 1
Вузол 2
Вузол 3
Вузол 4
Вузол 5
Блокчейн
Користувач
Кеш
Загальний кеш кореня дерева Меркла користувача
Загальний кеш кореня дерева Меркла для ролі


12
МЕТОД БАЛАНСУВАННЯ
ДЛЯ КЕРУВАННЯ ДАНИМИ
Аналіз поточної архітектури DApp
Децентралізація логіки між смарт-контрактами
Визначення ролей і формування дерев Меркла
Користувачі
Формування мережі блокчейн
Файлове сховище
Підключення балансувальника навантаження
Прийом поточної події
Тип події?
Додавання вузлу
Додавання файлу
Відновлення даних
Покинення вузлів
Алгоритм LRU
Вибір VC
Функція FSR
Аналіз кешу
Кількість VD
Розосередження
Оновлення VD
Корекція кешів, індексів та дерев Меркла

РЕЗУЛЬТАТИ ТЕСТУВАННЯ

13

Затримка передачі інформації про файли (сек)

		Min	Max	Ava	Median
Hyperledger	Завантажити	0.535	21.762	1.242023	0.585
	Скачати	0.27	16.615	0.927483	0.432
Hyperledger / Besu	Завантажити	2.21	12.214	3.203192	3.294
	Скачати	1.937	26.012	2.986525	2.902
Ropsten	Завантажити	3.512	388.917	27.27899	11.935
	Скачати	1.142	13.673	1.597874	1.258

Середній час тестування

Назва тіста	Необхідний час (мс)	Цільові показники (мс)
Додавання вузла	974	5000
Додавання одного файлу	1512	3000
Відновлення даних з втрачених вузлів	65 041	600 000
Відновлення вузла	1062	60 000

Результат тестування продуктивності

Тест (вимірюється в мс)	DecStore		Блокчейн	Централізований сервер (цільові показники)
	JSON	SQLite		
Надання нового дозволу файлу	157	190	100	60
Повна заборона доступу користувача	330	330	300	60
Перевірка доступу	130	140	100	10

ВИСНОВКИ

14

Сукупність отриманих у кваліфікаційній роботі результатів дозволило вирішити актуальне науково-технічне завдання, спрямоване на підвищення продуктивності децентралізованих систем на базі смарт-контрактів.

В результаті проведених досліджень отримані такі результати:

1. Проведений аналіз сучасного стану вирішення питань підвищення ефективності розподілу даних і керування доступом до них в децентралізованих системах.

2. Визначені підходи до розподілу даних в децентралізованих системах. Наведений метод, який дозволяє розподіляти дані по вузлах із мінімізацією місця зберігання.

3. Визначені підходи до контролю доступу в децентралізованих системах зберігання даних. Розглянута система контролю доступу, яка може працювати з блокчейном в поєднанні з локальним сховищем і механізмом кешування на боці користувачів. .

4. Удосконалений метод балансування для керування даними на базі смарт-контрактів за рахунок формування гібридної архітектури системи, де частина даних зберігається в блокчейн, а частина в локальних сховищах вузлів системи, що дозволило підвищити продуктивність децентралізованої інформаційної системи.

15

ПУБЛІКАЦІЯ У ФАХОВОМУ ЖУРНАЛІ КАТЕГОРІЇ «Б»


Системи управління, навігації та зв'язку

Control, navigation and communication systems

Випуск 1 (79)

Issue 1 (79)