

Практичне завдання №1:

Реалізація локального блокчейну

Опис:

Реалізуйте локальну версію блокчейну, яка буде працювати без децентралізації, але міститиме основні складові технології: блоки, хешування, майнінг та зв'язки між блоками.

Вимоги:

1. Клас **Block**:

- Кожен блок повинен містити наступні поля:
 - **index**: порядковий номер блоку.
 - **timestamp**: час створення блоку.
 - **data**: дані або транзакції, які містяться в блоці.
 - **previous_hash**: хеш попереднього блоку.
 - **hash**: унікальний хеш поточного блоку.
 - **nonce**: число, що використовується для майнінгу блоку.
- Реалізуйте метод для обчислення хешу блоку, використовуючи SHA-256 або інший хеш-алгоритм.

2. Клас **Blockchain**:

- Реалізуйте клас для блокчейну, який буде зберігати послідовність блоків.
- Блокчейн повинен мати метод для створення генезис-блоку (першого блоку в ланцюгу).
- Повинен бути метод для додавання нових блоків до блокчейну.
- Реалізуйте механізм майнінгу, де новий блок додається до блокчейну тільки після того, як хеш блоку відповідатиме заданому рівню складності (хеш повинен починатися з певної кількості нулів).

3. Майнінг блоків:

- Реалізуйте метод майнінгу, який змінюватиме значення **nonce**, поки не буде знайдено хеш, що відповідає умовам складності.
- Після майнінгу блоку виводьте на екран повідомлення з інформацією про хеш нового блоку.

4. Тестування:

- Створіть декілька блоків і додайте їх до блокчейну.
- Виведіть інформацію про всі блоки (номер, дані, хеш, попередній хеш, ...).

Додаткові завдання (опціонально):

- Додайте до блокчейну підтримку простих транзакцій.
- Реалізуйте перевірку цілісності блокчейну — функцію, яка перевірятиме правильність зв'язку між блоками за допомогою їх хешів.

Умови:

- Мова програмування: будь-яка зручна (Python, JavaScript, Java, C++ або інша).
- Виконання завдання повинно включати створення всіх основних компонентів блокчейну (блоки, ланцюг блоків, майнінг, хешування).
- Ви повинні протестувати роботу програми, додавши декілька блоків у ланцюг та перевіривши їхню коректність.

Очікуваний результат:

- Робоча програма, яка демонструє додавання нових блоків до ланцюга через процес майнінгу.
- Кожен блок повинен містити правильний хеш, пов'язаний із попереднім блоком.
- Лог програми, який показує процес майнінгу і структуру блоків.

Додаткова інформація Алгоритм Proof of Work

Опис:

Однією з ключових складових вашої локальної реалізації блокчейну є майнінг. У цьому завданні майнінг реалізується через алгоритм Proof of Work (PoW) — механізм, який вимагає від вузлів мережі (в даному випадку, вашої програми) вирішення складної математичної задачі для додавання нового блоку до блокчейну.

Цей алгоритм гарантує, що кожен новий блок буде доданий після значної обчислювальної роботи, що забезпечує безпеку та незмінність даних у ланцюзі.

Що таке Proof of Work (PoW):

Proof of Work — це алгоритм консенсусу, який забезпечує узгодженість між вузлами блокчейну. Основна ідея полягає в тому, що для додавання нового блоку до ланцюга майнери повинні вирішити складну задачу: знайти такий параметр **nonce** (спеціальне число), який разом з іншими даними блоку генерує хеш, що відповідає певній умові — починається з певної кількості нулів.

Алгоритм майнінгу:

1. Складність майнінгу:

- Складність майнінгу визначається числом нулів, з яких повинен починатися хеш нового блоку. Чим більше нулів, тим складніше знайти правильний хеш.
- Наприклад, якщо складність дорівнює 4, то хеш нового блоку повинен починатися з чотирьох нулів: 0000xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.

2. Процес майнінгу (Proof of Work):

- Для додавання нового блоку програма повинна знайти такий **nonce**, який у поєднанні з іншими даними блоку дасть хеш, що починається з певної кількості нулів.
- Програма генерує новий хеш кожного разу, змінюючи значення **nonce**, поки не знайде такий хеш, що відповідає умові складності.

3. Алгоритм майнінгу:

- Програма змінює значення **nonce** і обчислює хеш.
- Якщо хеш не відповідає умові складності, **nonce** збільшується, і обчислення повторюється.
- Процес триває, поки не буде знайдено правильний хеш.
- Після успішного майнінгу програма повідомляє, що блок було успішно здобуто.