# ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

**Харківський національний університет радіоелектроніки**

**Кафедра ЕОМ**

# Метод федеративного навчання на основі блокчейн

Виконав ст.групи СПм-22-6
Бохан І.А.

Керівник
Доц.каф.ЕОМ Ляшенко О.С.

## Актуальність, мета та задачі роботи

Федеративне навчання (FL) – це новий метод машинного навчання, у якому всі учасники можуть спільно навчати модель, не передаючи свої необроблені дані, таким чином розбиваючи дані й уникаючи проблем конфіденційності, спричинених централізованим зберіганням даних

**Мета кваліфікаційної роботи** полягає в реалізації метода федеративного навчання на основі блокчейн

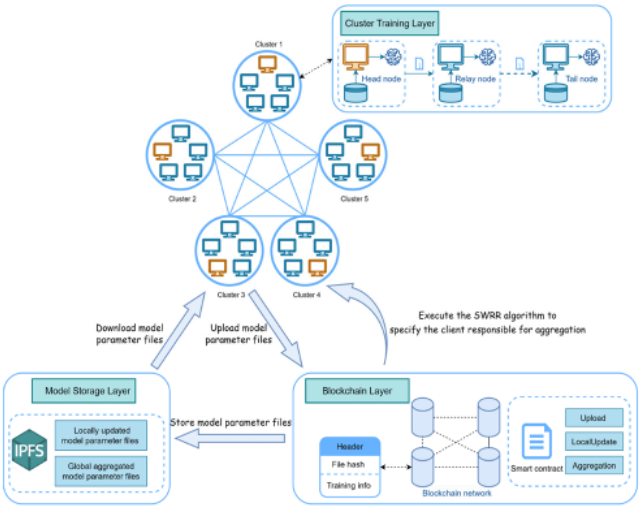
**Задачі**

- Побудувати архітектуру методу BCFL
- Дослідити процес зберігання параметрів моделі
- Розробити смарт-контракт необхідний до нашої системи
- Провести тестування та оцінювання

# Архітектура системи BCFL

В роботі застосовано блокчейн і IPFS до архітектури FL на основі алгоритму навчання кластера з парним і непарним циклом і поєднує операції розрідженого квантування параметрів моделі зі структурою сітчастої топології для подальшого підвищення ефективності зв'язку, забезпечуючи при цьому надійність FL. Як показано на рисунку, децентралізована архітектура BCFL складається з наступних рівнів:

- рівня навчання кластера,
- рівня блокчейну
- рівня зберігання моделі.




## Запис процесу федеративного навчання

### Ланцюжок консорціуму

BCFL представляє ланцюжок консорціуму для запису процесу FL, забезпечуючи прозорість та надійність.

### Оптимізація зберігання

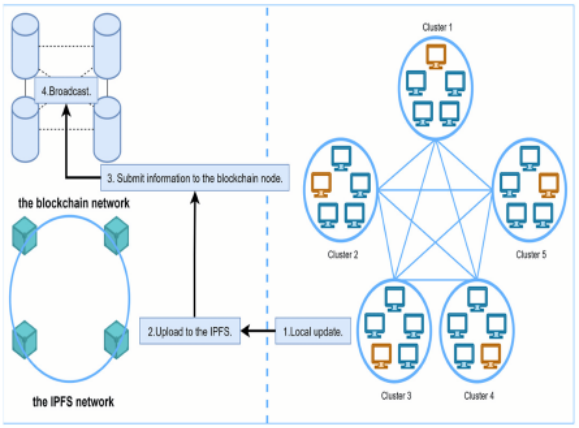
Проблема великих накладних витрат на зберігання ланцюга консорціуму вирішується шляхом поєднання з IPFS.

# Зберігання параметрів моделі

Зберігання та оновлення параметрів моделі особливо важливі, і в цьому розділі описано режим зберігання, який поєднує ланцюг консорціуму з IPFS для зберігання параметрів моделі об'єднаного навчання.

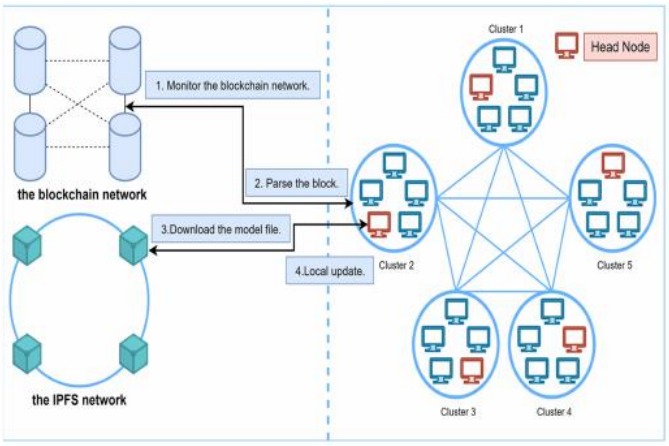
Процес розділений на три етапи: ініціалізація, збереження параметрів моделі та синхронізація параметрів моделі. Ініціалізація: налаштуйте ланцюжок консорціуму, одночасно запустіть вузол IPFS і приєднайтеся до мережі IPFS.

Зберігання параметрів моделі: у кожному раунді об'єднаного навчання учасники оновлюють параметри моделі на основі своїх локальних даних, а оновлені параметри моделі зберігаються в мережі IPFS. Конкретні кроки показано на рисунку.




Принципова схема зберігання параметрів моделі.

# Діаграма синхронізації параметрів моделі




Синхронізація параметрів моделі: щоб гарантувати, що головний вузол у кожному кластері може своєчасно отримувати останні параметри моделі, необхідно розробити механізм синхронізації. На рисунку показано процес синхронізації.

# Розробка смарт-контракту

Для реалізації нашого метода потрібно реалізувати смарт-контракт який відповідає за виконання основних функцій, таких як завантаження моделі, локальне оновлення та глобальне агрегування моделі. Рівень смарт-контракту включає три ключові функції: *Upload( ), LocalUpdate( ), Aggregation( )*

1

**Функція Upload()**

*Upload( )* функція відповідає за реалізацію завантаження параметрів моделі, яка виконується клієнтом-учасником у процесі навчання.

2

**Функція LocalUpdate()**

Функція *LocalUpdate()* відповідає за обробку оновлення локальної моделі та виконується клієнтами, які беруть участь у процесі навчання.

3

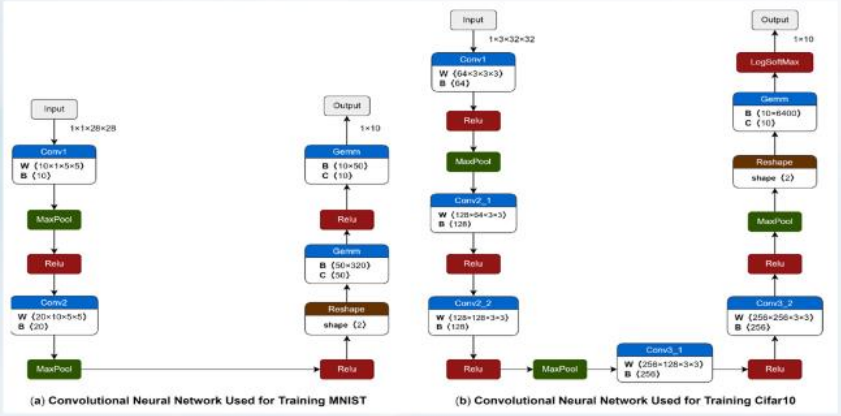
**Функція Aggregation()**

Функція *Aggregation()* відповідає за обробку глобальної агрегації моделі

# Експериментальне тестування

1 **Постановка та впровадження експерименту**

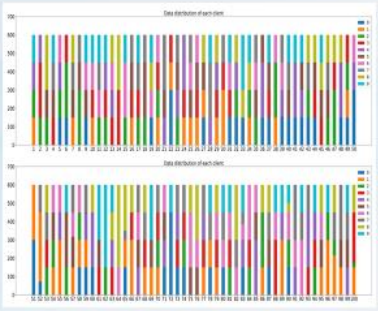
У цьому експерименті використовувалися моделі нейронних мереж, показані на рисунку, для навчання наборів даних MNIST і CIFAR-10.



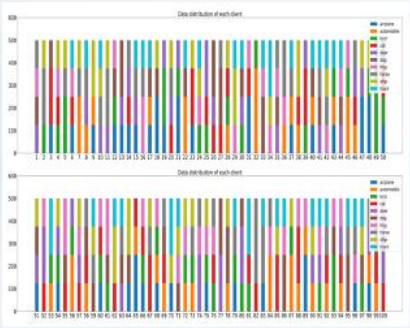
# Експериментальне тестування

**2** **Моделювання різних сценаріїв**

Для моделювання різних сценаріїв даних, навчальний набір даних був відсортований за мітками та розділений на 400 рівних частин. Під час тренінгу FL кожен із 100 клієнтів-учасників випадковим чином обирає чотири частини. На рисунках - гістограми представляють розподіл міток наборів даних MNIST і CIFAR-10, зайнятих 100 клієнтами. Різні кольори на гістограмах представляють різні типи міток у наборах даних.



MNIST



CIFAR-10

# Експериментальне тестування

**3** **Параметри обробки параметрів моделі для BCFL**

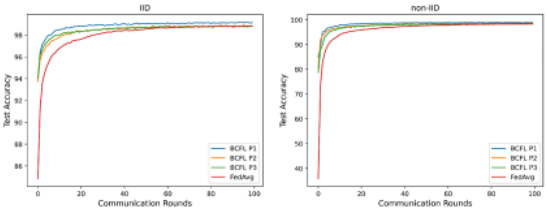
В експериментальних умовах необхідно розглянути, чи є параметри моделі розрідженими, і в цьому експерименті було обрано коефіцієнт розрідженості 0,5. У той же час, також необхідно розглянути питання про квантування значень параметрів моделі від чисел з плаваючою комою повної точності до чисел половинної точності. Таким чином, для встановлення параметрів моделі в BCFL було використано три методи обробки, які наведено в таблиці

| Pattern | Використовується розрідженість? | Використовується квантування? |
|---|---|---|
| Шаблон 1 (P1) | ні | ні |
| Шаблон 2 (P2) | так | ні |
| Шаблон 3 (P3) | так | так |

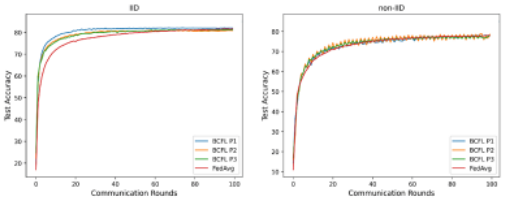
# Аналіз точності та вартості зв'язку

Були проведені експерименти з двома розподілами даних MNIST і CIFAR-10, щоб перевірити ефективність навчання фреймворку BCFL на алгоритмічному рівні в FL. Алгоритм FL, який найчастіше використовується, FedAvg, порівнювався з BCFL за різними шаблонами обробки параметрів.

Під час аналізу вартості зв'язку розглядалася лише передача файлів параметрів моделі між клієнтами, де комунікація вгорі відноситься до передачі файлів параметрів моделі в межах кластера, а зв'язок у низхідній частині стосується глобального файлу параметрів моделі, який передається вузлом агрегатора головний вузол кожного кластера. Результати експерименту набору даних MNIST показано на рисунку




Результати експерименту набору даних CIFAR-10.




# Висновки

У цій роботі пропонується метод об'єднаного навчання, заснований на непарно-парному навчанні кластера. Розділивши клієнтів на кластери та застосувавши частково серіалізований метод навчання в кластерах, ми можемо прискорити конвергенцію моделі. Перед передачею параметрів файл моделі розріджується та квантується, щоб зменшити витрати на зв'язок і підвищити ефективність зв'язку FL.

Архітектура BCFL більше не покладається на центральний сервер і використовує алгоритм балансування навантаження для планування клієнта, відповідального за агрегацію, у кожному раунді. Він представляє ланцюжок консорціуму для запису процесу FL і оптимізує проблему великих накладних витрат на зберігання ланцюга консорціуму шляхом поєднання з IPFS.

Експерименти з наборами даних MNIST і CIFAR-10 демонструють, що запропонована структура відрізняється точністю та ефективністю зв'язку, а аналіз часу показує, що запропонована модельна схема обробки файлів є корисною для підвищення ефективності передачі FL. Незважаючи на те, що ця робота має певні досягнення в оптимізації продуктивності FL і проектуванні децентралізованої архітектури, все ще є багато напрямків для подальших досліджень і вдосконалень.

# Публікація

Подана стаття в науковий журнал «СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ І ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ»
Ляшенко О.С., Бохан І.А., Крюкова І.В. **Метод федеративного навчання на основі блокчейн**
Вихід збірника статей планується на липень місяць 2024 р.