

ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

КАФЕДРА ЕОМ
КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

«Програмні компоненти для токенизації освітніх активів на основі
смарт-контрактів Ethereum»

Керівник: доц. Каф. Олександр ШМАТКО

Виконав: здобувач Олексій ЛІЗУНОВ

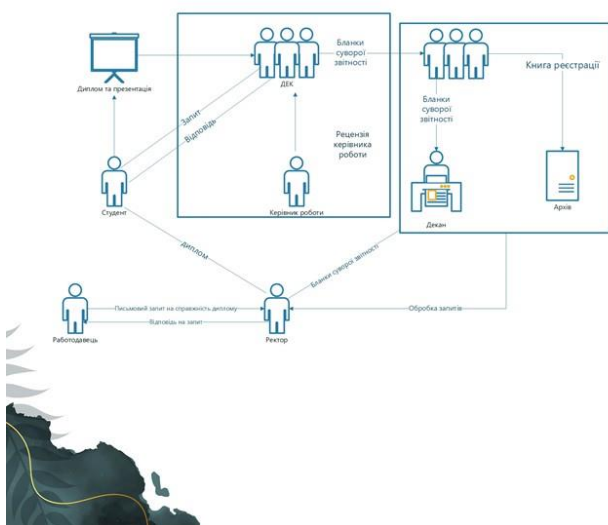
МЕТА ТА ПОСТАНОВКА ЗАВДАННЯ

Метою кваліфікаційної роботи є дослідження, проектування та розробка програмних компонентів для токенизації освітніх активів з використанням блокчейн-технологій на платформі Ethereum. Цей процес включає використання смарт-контрактів, технологій Web3 та клієнтської частини на базі React.js.

У межах поставленої мети необхідно вирішити такі завдання:

- Провести аналіз методів забезпечення конфіденційності та цілісності даних у блокчейн-системах;
- Дослідити принципи функціонування хеш-алгоритмів у контексті захисту даних;
- Розглянути інструменти збереження приватності в децентралізованих реєстрах;
- Розробити прототип децентралізованого застосунку для токенизації освітніх активів на основі Ethereum;
- Провести тестування системи та оцінити її придатність до практичного впровадження.

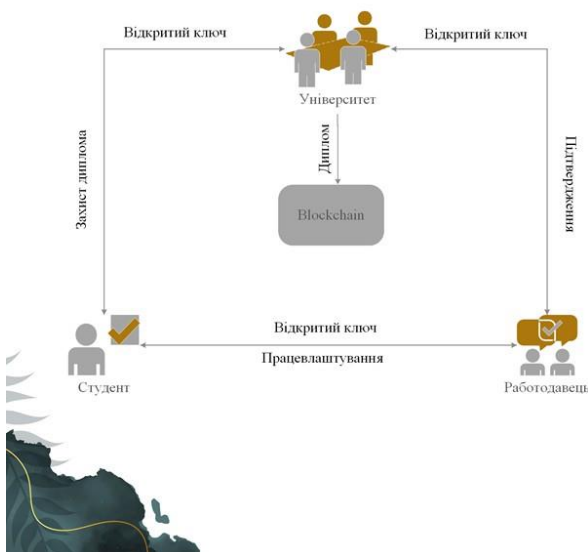
АКТУАЛЬНІСТЬ ПРОЕКТУ



- складність перевірки справжності документів;
- ризики фальсифікації дипломів і сертифікатів;
- залежність від роботи централізованих реєстрів;
- обмежений доступ до інформації про навчальні досягнення студентів;
- високі витрати на адміністрування та верифікацію даних.

3

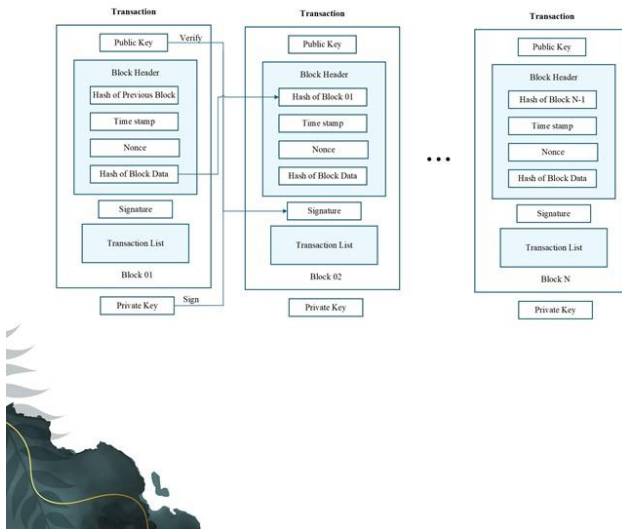
Трансформаційний потенціал блокчейну в освіті



- Повний контроль над цифровою ідентичністю, створення портфоліо.
- Неможливість підробки, захист даних через хеші та ZKP.
- Легка перевірка документів, зниження адміністративного навантаження.
- Незалежність від локального зберігання, доступність даних.
- Автоматизація видачі дипломів, зменшення посередників.

4

Структура блокчейна для зберігання освітніх даних

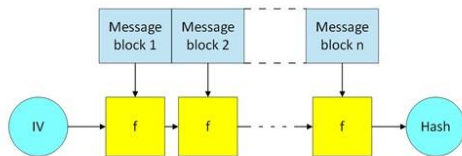


Принципи збереження даних:

- Після запису інформація не може бути змінена або видалена без нового блоку.
- Будь-хто може перевірити, що освітній запис дійсно існує.
- IPFS-хеш дозволяє підтвердити, що документ не змінено.
- За потреби — ZKP (Zero-Knowledge Proofs) можуть забезпечити перевірку без розкриття персональних даних.

5

Хешування та захист даних



- Завжди генерує 256-бітний (32-байтний) хеш, незалежно від розміру вхідних даних.
- Однакові вхідні дані завжди дають однаковий результат.
- Практично неможливо відновити оригінальні дані, знаючи лише хеш.
- Ймовірність того, що різні вхідні дані створять однаковий хеш, є надзвичайно низькою.
- Навіть мінімальна зміна у вхідних даних призводить до кардинально іншого хешу.

Zero-Knowledge Proof



Криптографічний метод, що дозволяє підтвердити достовірність твердження без розкриття самої інформації.
Приклад: Студент може довести наявність диплому, не надаючи його PDF, номер чи назву вишу.

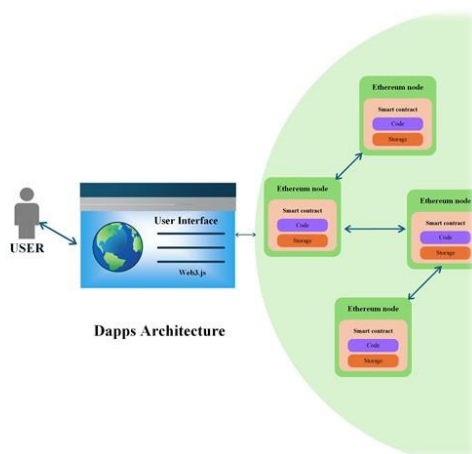
6

Ключові технології токенизації освітніх активів

- Ethereum: Децентралізована платформа для смарт-контрактів та DApps. EVM, Solidity, стандарти токенів (ERC-20, ERC-721, ERC-1155).
- Ethereum 2.0 (PoS) та Layer 2 рішення: Масштабованість, зниження комісій (Rollups, Sidechains).
- Ethereum Name Service (ENS): Децентралізована система доменних імен для зручної ідентифікації (ivanov.eth).
- Self-Sovereign Identity (SSI): Концепція самостійного управління даними (DID, Verifiable Credentials, Wallet SSI).
- DAO (Decentralized Autonomous Organization): Децентралізоване управління освітніми проєктами.
- Zero-Knowledge Proofs (ZKP): Підтвердження інформації без її розкриття – для конфіденційності дипломів.

7

Архітектура децентралізованого додатку



На рисунку представлено загальну архітектуру децентралізованого додатку, розгорнутого у середовищі Ethereum.

Ця архітектура демонструє, як користувач, не маючи прямого доступу до блокчейну, взаємодіє з децентралізованою системою через зручний UI, а дані, дії та транзакції обробляються в trustless-середовищі Ethereum без центрального посередника.

Цю модель можна використати як основу для освітніх платформ, які дозволяють зберігати дипломи, сертифікати, результати тестувань тощо у формі токенів або записів у смарт-контрактах.

8

Інтерфейс користувача

