

УДК 004

Жмуцький М.А.¹, Олійник А.О.²

¹ студ. гр. КНТ-124м НУ «Запорізька політехніка»

² проф. НУ «Запорізька політехніка»

ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ НА ОСНОВІ БЛОКЧЕЙНУ ДЛЯ ВЕРИФІКАЦІЇ ДОКУМЕНТІВ

Об'єкт дослідження – процес розробки програмного забезпечення для верифікації документів з використанням блокчейн-технологій.

Предмет дослідження – методи та програмні засоби децентралізованої ідентифікації W3C DID та верифікації документів через криптографічні хеші SHA-256, смарт-контракти Ethereum та IPFS.

Мета роботи – розробка децентралізованої програмної системи верифікації документів для підвищення швидкості перевірки та безпеки від підробки.

Актуальність: традиційна верифікація займає дні-тижні, вразлива до підробки, має єдину точку відмови, порушує приватність користувачів.

Матеріали та засоби: JavaScript/Node.js 18, React 18.2, Solidity 0.8.19, Ethers.js 6.4, IPFS, MongoDB 6.0, Hardhat, MetaMask, SHA-256; ПК: Intel i5-12500H, 16 ГБ RAM.

У результаті роботи було розроблено децентралізовану систему верифікації академічних документів на основі блокчейн-технологій, IPFS та децентралізованих ідентифікаторів, яка дозволяє здійснювати операції видачі, зберігання та перевірки автентичності освітніх документів без залежності від централізованих органів.

Для досягнення мети було вирішено ряд завдань: досліджено проблеми традиційної верифікації академічних документів, включаючи тривалість процедури, високу вартість та ризики підробки; проаналізовано особливості децентралізованих систем ідентифікації та розподіл відповідальності між учасниками; вивчено стандарти W3C Verifiable Credentials та W3C DID для

забезпечення міжнародної сумісності; оцінено існуючі рішення та виявлено їх недоліки.

Наукова новизна роботи полягає у тому, що запропоновано модель гібридного зберігання даних для децентралізованої системи верифікації академічних документів, яка поєднує три рівні: приватну блокчейн-мережу Ethereum з консенсусом Proof-of-Authority для незмінного реєстру криптографічних хешів документів, децентралізоване сховище IPFS для повного вмісту документів у форматі W3C Verifiable Credentials та документо-орієнтовану базу даних MongoDB з TTL-індексами для операційних даних і багаторівневого кешування. Також розроблено модель послідовності операцій смарт-контракту з механізмом ізоляції емітентів через контроль доступу на основі авторизованих адрес, що забезпечує незалежне функціонування університетів-емітентів з власними DID-ідентифікаторами та криптографічними ключами без можливості модифікації записів інших учасників системи. Запропонована архітектура дозволяє досягти балансу між децентралізацією через незмінність критичних записів у блокчейні, продуктивністю з часом верифікації менше п'яти секунд для некешованих запитів та економічною ефективністю завдяки нульовим витратам на gas у приватній мережі, а також забезпечує захист від несанкціонованого доступу через механізм ізоляції емітентів на рівні смарт-контракту.

Розроблене програмне забезпечення підтримує функціонування необмеженої кількості університетів-емітентів в ізольованому форматі, де кожен емітент має власний DID-ідентифікатор та криптографічні ключі. Відповідальність у системі розподілена між трьома ролями: емітент може видавати верифіковані документи згідно зі специфікацією W3C VC через веб-інтерфейс з автоматичною реєстрацією в блокчейні, завантаженням до IPFS та відкликанням документів у випадку виявлення помилок; власник документів може переглядати всі свої академічні кваліфікації в єдиному інтерфейсі, самостійно перевіряти їх валідність та створювати безпечні способи обміну з верифікаторами через IPFS CID, QR-коди або прямі посилання; верифікатор може перевіряти автентичність документів за кілька секунд через введення IPFS CID або завантаження JSON-файлу з детальним відображенням результату кожного етапу перевірки, включаючи валідацію структури, порівняння хешів, перевірку статусу в блокчейні та верифікацію цифрових підписів.

Архітектура системи побудована на принципах децентралізації та Self-Sovereign Identity, що надає користувачам повний контроль над своїми даними. Використання блокчейн-технології забезпечує незмінність записів про документи та прозорість процесу верифікації. Децентралізоване сховище IPFS гарантує доступність повного вмісту документів без залежності від окремих серверів. Криптографічні методи захисту, включаючи SHA-256

хешування та цифрові підписи на еліптичній кривій secp256k1 , забезпечують високий рівень безпеки від підробки документів.

Тестування системи підтвердило коректність роботи всіх компонентів з успішним проходженням тринадцяти модульних тестів для серверних сервісів, дванадцяти тестів смарт-контракту та восьми інтеграційних тестів основних сценаріїв використання. Перевірка сумісності показала повну підтримку в браузерях Chrome, Firefox та Edge, а також часткову підтримку в Safari з необхідністю додаткового налаштування MetaMask. Система демонструє прийнятну продуктивність з часом верифікації документа менше п'яти секунд для некешованих запитів та менше однієї секунди для кешованих даних завдяки впровадженому методу багаторівневого кешування.

Розроблений програмний продукт дозволяє університетам скоротити адміністративні витрати на обробку запитів про підтвердження документів, випускникам мати постійний доступ до своїх академічних кваліфікацій незалежно від стану університету, а роботодавцям швидко перевіряти кваліфікації кандидатів без затримок у процесі найму. Децентралізована природа системи забезпечує її стійкість до відмов окремих компонентів та захист від втрати даних через розподілене зберігання в блокчейні та IPFS-мережі, що сприяє покращенню довіри до процесу верифікації академічних документів та підвищенню ефективності ринку праці.

Перспективи подальшого розвитку системи включають впровадження селективного розголошення атрибутів через zero-knowledge proofs для захисту приватності, інтеграцію з міжнародними реєстрами акредитованих університетів, розширення функціональності для підтримки інших типів документів поза академічною сферою, а також оптимізацію витрат на gas через використання layer-2 рішень або sidechains для масштабування системи на глобальному рівні.

Галузь використання: університети для видачі дипломів, роботодавці для перевірки кваліфікацій, медзаклади для сертифікатів, HR-департаменти для швидкого найму.