DOI https://doi.org/10.32689/maup.it.2026.2.5
УДК 004.056:378
JEL Classification: I23, K24, O33

АРХІТЕКТУРА ЗАХИЩЕНОЇ КОНСОРЦІУМНОЇ ВИДАЧІ БЛОКЧЕЙН-СЕРТИФІКАТІВ З ДОТРИМАННЯМ ЄВРОПЕЙСЬКИХ ВИМОГ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ

О. А. Нємкова, А. М. Ахекян

SECURE CONSORTIUM-BASED BLOCKCHAIN CERTIFICATE ISSUANCE ARCHITECTURE COMPLIANT WITH EUROPEAN PERSONAL DATA PROTECTION REQUIREMENTS FOR E-LEARNING SYSTEMS

Elena Nyemkova, Artem Akhekian

Анотація

Об'єктом дослідження є системи блокчейн-сертифікації освітніх досягнень у e-learning. За даними HireRight Global Benchmark Report (2025), до 47 % роботодавців у регіоні EMEA фіксують розбіжності в освітніх документах кандидатів під час перевірки, що обґрунтовує актуальність теми. Проблема, що вирішувалася: наявні блокчейн-рішення архітектурно розраховані на одного видавця, не пропонують механізму узгодження незмінності реєстру з правом на видалення персональних даних за GDPR (ст. 17) та не мають методики інтеграції з LMS. Отримано архітектурну модель та прототип консорціумної системи CertificateRegistry, що поєднує поділ даних на незмінний on-chain хеш (SHA-256, Merkle Root) та off-chain сховище персональних даних, яке можна видалити; рольовий контроль доступу з розмежуванням ролей видавця та адміністратора, що дозволяє одному реєстру обслуговувати консорціум університетів; методику інтеграції з LMS Moodle через Webhooks, REST API та стандарт LTI 1.3. Застосовано поєднання даних механізмів у єдиній архітектурі контракту, тоді як у відомих рішеннях вони реалізовувались окремо або не реалізовувались взагалі. При видаленні off-chain даних on-chain хеш перетворюється на «сироту», яка не ідентифікує особу, знімаючи суперечність між незмінністю реєстру та правом на забуття. Прототип пройшов unit-тестування (15 тест-кейсів) та функціональне тестування в мережі Ethereum Sepolia; розрахункова вартість видачі сертифіката на Polygon PoS становить $0,00001, користувацьке тестування підтвердило зростання точності виявлення підробок з 66,7 % до 100 %, а показник зручності використання порталу (SUS) склав 82,5 зі 100 балів. Результати можуть використовуватися консорціумами закладів вищої освіти, що працюють на базі Moodle у правовому полі Європейського Союзу, для впровадження верифікованих цифрових сертифікатів без істотних інфраструктурних витрат.

Ключові слова: *блокчейн, смарт-контракт, GDPR, сертифікат, контроль доступу, консорціум, e-learning, Moodle.*

Abstract

The object of research is blockchain-based certification systems for educational achievements in e-learning. According to the HireRight Global Benchmark Report (2025), up to 47% of employers in the EMEA region identify education-credential discrepancies during screening, confirming the topic's relevance. Existing blockchain solutions target a single issuer, lack a mechanism reconciling ledger immutability with the GDPR right to erasure (Art. 17), and lack an LMS integration methodology. An architectural model and prototype of a consortium CertificateRegistry system were developed, combining: separation of data into an immutable on-chain hash (SHA-256, Merkle Root) and an erasable off-chain personal-data store; role-based access control separating issuer and administrator roles, enabling one registry to serve a university consortium; and a methodology for Moodle LMS integration via Webhooks, REST API and LTI 1.3. Known solutions implement these mechanisms separately or not at all; here they are combined in one contract architecture. Deleting off-chain data turns the on-chain hash into an «orphan» that no longer identifies a person, removing the contradiction between immutability and the right to erasure. The prototype passed unit testing (15 test cases) and functional testing on Ethereum Sepolia; the calculated cost of certificate issuance on Polygon PoS is $0.00001, user testing showed fraud-detection accuracy rising from 66.7% to 100%, and portal usability (SUS) reached 82.5 of 100. The results can be applied by consortia of higher education institutions on Moodle within the EU legal framework to deploy verifiable digital certificates without significant infrastructure costs.

Key words: *blockchain, smart contract, GDPR, certificates, access control, consortium, e-learning, Moodle.*

1. Вступ. Масове поширення цифрових освітніх облікових даних (сертифікатів, мікрокредентіалів, транскриптів) перетворило їхню верифікацію на самостійну задачу забезпечення цілісності та автентичності даних поза межами довіри до єдиного центрального органу. За даними HireRight Global Benchmark Report (2025), заснованого на щорічному опитуванні понад 1000 HR-фахівців у світі, розбіжності в освітніх документах кандидатів є однією з найпоширеніших знахідок під час перевірки – до 47 % випадків у регіоні EMEA (Europe, Middle East and Africa) [1]. Це не лише проблема довіри до окремого документа, а проблема інформаційної безпеки в масштабі галузі: традиційна верифікація покладається на доступність і сумлінність видавця, що створює єдину точку відмови та робить систему

© Нємкова О. А., Ахекян А. М., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

вразливою до підробки, відмови видавця в обслуговуванні та припинення його діяльності. Блокчейн-технологія усуває залежність від доступності видавця за рахунок криптографічно верифіковного, розподіленого запису [2], проте перенесення цієї технології в освітній контекст породжує власну проблему безпеки даних: незмінність реєстру, що є джерелом довіри до системи, прямо суперечить вимозі права на видалення персональних даних (ст. 17 GDPR, Загальний регламент захисту даних, англ. General Data Protection Regulation) [3]. Розв'язання цього конфлікту на рівні архітектури, а не декларативно, є необхідною умовою для впровадження blockchain-сертифікації в юрисдикціях, що підпадають під дію GDPR, – а отже, дослідження, присвячені технічному узгодженню незмінності блокчейну з вимогами захисту персональних даних у сценарії багатьох незалежних видавців, є актуальними.

Аналіз наукових джерел останніх років дозволяє виділити три групи робіт, релевантних поставленій проблемі.

Перша група – узагальнюючі дослідження застосування блокчейну в освіті [4],[5],[6],[7], а також концептуальні освітні платформи на кшталт Kudos [8] та EduCTX [9]. Ці роботи обґрунтовують доцільність блокчейн-сертифікації на рівні архітектурної концепції, проте не пропонують інженерного рішення конфлікту між незмінністю реєстру та правом на видалення персональних даних: питання GDPR або не розглядається взагалі, або згадується як обмеження без запропонованого технічного механізму розв'язання. Це залишає розробників без відтворюваного архітектурного патерна для юрисдикцій ЄС.

Друга група – реалізовані системи видачі блокчейн-сертифікатів одному видавцю: модель довіри Lizcano та ін. [10], а також новітні прототипи 2023–2025 рр. на базі альтернативних мереж. Спільна риса цих рішень – архітектура розрахована на єдиного видавця; механізми контролю доступу, якщо присутні, не передбачають сценарію, коли кілька незалежних закладів освіти видають сертифікати в межах одного спільного реєстру. Це узгоджується з висновком систематичного огляду літератури з блокчейн-верифікації академічних сертифікатів, який прямо відносить низьку взаємосумісність між закладами освіти до головних обмежень наявних моделей [11]. Об'єктивна причина цього обмеження – більшість прототипів створювалися як proof-of-concept для одного навчального закладу, а не як інфраструктурне рішення для консорціуму.

Третя група – роботи зі стандартизації цифрових облікових даних: W3C Verifiable Credentials [12], Open Badges 3.0 [13], Blockcerts [14],[15]. Вони вирішують проблему сумісності формату сертифіката між платформами, проте залишають відкритим питання операційної інтеграції сервісу видачі з конкретною системою управління навчанням (LMS): описані у стандартах верифікаційні портали розглядаються як ізольовані застосунки, без визначення механізму отримання події про завершення курсу, резервного каналу за відмови основного, чи вбудовування в інтерфейс LMS. Причина цієї прогалини суб'єктивна: специфікації навмисно залишаються platform-agnostic, тому питання конкретної інтеграції з LMS свідомо виноситься за межі стандарту.

Систематизація виявлених обмежень дозволяє сформулювати загальну невирішену проблему: наявні блокчейн-системи сертифікації в освіті архітектурно розраховані на одного видавця, не пропонують технічного механізму узгодження незмінності реєстру з правом на видалення персональних даних за GDPR та не мають відтворюваної методики інтеграції з операційним циклом конкретної LMS, що обмежує їх застосовність для консорціумів закладів освіти, які діють у правовому полі ЄС.

Метою дослідження є розроблення архітектурної моделі та методики контролю доступу для консорціумної видачі й верифікації блокчейн-сертифікатів, яка технічно узгоджує незмінність реєстру з вимогами GDPR щодо права на видалення персональних даних. Це дасть можливість створити відтворюваний прототип системи видачі та верифікації сертифікатів з готовою інтеграцією в LMS Moodle, придатний для пілотного впровадження консорціумом закладів вищої освіти.

Для досягнення мети були поставлені наступні задачі:

– систематизувати підходи до узгодження незмінності блокчейну з правом на видалення персональних даних (ст. 17 GDPR) у наявних рішеннях та обґрунтувати архітектурний патерн їх розв'язання;

– розробити модель рольового контролю доступу для консорціумного сценарію видачі сертифікатів кількома незалежними видавцями в межах одного реєстру;

– спроектувати та реалізувати смарт-контракт CertificateRegistry, що відповідає сформульованим вимогам GDPR-сумісності та консорціумного доступу;

– розробити методику інтеграції сервісу видачі сертифікатів з LMS Moodle на рівні подій, REST API та стандарту LTI 1.3 (Learning Tools Interoperability);

– провести тестування прототипу (unit-, функціональне, користувацьке) та оцінити економічну доцільність запропонованого рішення.

2. Матеріали і методи. Об'єктом дослідження є системи цифрової сертифікації у e-learning.

Гіпотеза дослідження. Технічна сепарація незмінних криптографічних доказів (хешів документів, Merkle Roots) від персональних даних, що зберігаються off-chain, у поєднанні з рольовою моделлю

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

контролю доступу дозволяє побудувати блокчейн-реєстр сертифікатів, який одночасно відповідає вимозі GDPR щодо права на видалення персональних даних і придатний для обслуговування консорціуму незалежних видавців у межах єдиного смарт-контракту.

Припущення дослідження: заклади-учасники консорціуму довіряють спільному смарт-контракту та адміністратору, що надає роль ISSUER_ROLE (модель довіри є напівцентралізованою на рівні призначення ролей, тоді як сам реєстр залишається публічним і децентралізованим); студенти мають доступ до базового клієнтського програмного забезпечення (браузер, електронна пошта) для отримання та пред'явлення сертифіката; LMS підтримує механізм Webhooks або REST API для передачі подій про завершення курсу.

Спрощення, прийняті в роботі: прототип протестовано на обмеженій вибірці учасників (14 студентів, 6 HR-фахівців) та обмеженому розмірі пакета сертифікатів (до 100), що не відтворює навантаження масштабного промислового впровадження; економічний аналіз враховує лише вартість блокчейн-транзакцій без витрат на розробку, підтримку інфраструктури IPFS та навчання персоналу; оцінка безпеки контракту обмежена статичним аналізом (Slither, MythX) без незалежного зовнішнього аудиту.

Методи дослідження: аналіз наукової та технічної літератури; порівняльний аналіз блокчейн-платформ; архітектурне проектування; розробка смарт-контрактів мовою Solidity; тестування на Ethereum testnet (Sepolia). Теоретичну основу становлять: Bitcoin Whitepaper (Nakamoto, 2008) [2]; Ethereum Whitepaper (Buterin, 2014) [16]; W3C Verifiable Credentials Data Model 2.0 [12]; стандарт IMS Open Badges 3.0 [13]; Blockcerts v3 specification [14].

Практична значущість: розроблений смарт-контракт та портал верифікації є готовим відкритим рішенням (MIT ліцензія) для університетів та MOOC-платформ; описана методологія інтеграції з Moodle дозволяє впровадити систему без модифікації ядра LMS.

Прототип реалізовано у вигляді Node.js-сервісу (Certificate Issuer Service), інтегрованого з Moodle; смарт-контракту, розгорнутого в тестовій мережі Ethereum Sepolia, та порталу верифікації (React SPA). Для тестування обрано мережу Ethereum Sepolia, а не безпосередній наступник Polygon Mumbai **–** мережу Polygon Amoy, з огляду на довшу історію стабільної роботи Sepolia та ширшу базу документації й інструментів (Alchemy, Hardhat, MetaMask), за відсутності суттєвої різниці в поведінці EVM-сумісних смарт-контрактів між тестовими мережами. Мережу Polygon Mumbai було знято з обслуговування у 2024 р. Для промислової експлуатації рекомендується мережа Polygon PoS mainnet.

Технологічний стек: Solidity 0.8.20 – мова смарт-контрактів; Hardhat – фреймворк розробки та тестування; OpenZeppelin 5.0 [18] – бібліотека перевірених контрактних компонентів; ethers.js v6 – JavaScript-клієнт для взаємодії з блокчейном; IPFS (Pinata IPFS API) – зберігання JSON-сертифікатів; cert-issuer (Python, Blockcerts) – генерація сертифікатів у Blockcerts-форматі; React 18 + TypeScript – портал верифікації.

Pinata IPFS API обрано з огляду на керований (managed) хостинг без необхідності розгортання власного вузла, гарантоване закріплення файлів (persistent pinning), відкриту реєстрацію з безкоштовним тарифом та розвинений REST API й TypeScript SDK, сумісні з обраним технологічним стеком. Оскільки метою є демонстрація реалізованості запропонованої архітектури, а не прив'язка до конкретного постачальника, будь-який IPFS pinning-сервіс з еквівалентним функціоналом (Web3.Storage, NFT.Storage) може бути використаний як рівноцінна заміна без зміни архітектури системи.

Розгортання та конфігурація середовища виконуються через файл hardhat.config.ts.

Порівняльний аналіз блокчейн-платформ

На основі аналізу технічних характеристик, вартості розробки та впровадження проведено порівняльний аналіз чотирьох платформ для освітніх блокчейн-сертифікатів [16], [19], [5] (табл. 1).

Таблиця 1

Порівняльний аналіз блокчейн-платформ для освітніх сертифікатів

Критерій	Ethereum (L1)	Polygon (L2)	Hyperledger Fabric	Solana
Тип	Публічний	Публічний L2	Приватний/Консорц.	Публічний
Вартість транзакції	$0.05–$1	$0.001–$0.01	Нульова	$0.001
Пропускна здатність	15–30 TPS	2 100 + TPS	3 000+ TPS	2 100 + TPS
Децентралізація	Дуже висока	Висока	Низька	Середня
Зрілість/Безпека	Дуже висока	Висока	Висока	Середня
Blockcerts підтр.	Так	Так (EVM)	Частково	Ні
GDPR-відповідність	Складна	Складна	Гнучка	Складна
Рекомендується для	Публічні VC	Mass-adoption	Корпоратив/ВНЗ	Мікроплатежі

Для прототипу даної роботи обрано EVM-сумісний стек на основі Ethereum (Sepolia testnet для розробки й тестування, Polygon PoS mainnet для промислової експлуатації) з таких причин: EVM-сумісність дозволяє використовувати Solidity та Ethereum-інструменти без змін; вартість транзакції $0.001 на Polygon PoS є прийнятною навіть при видачі тисяч сертифікатів щорічно; підтримка Blockcerts формату; децентралізація та публічна верифікованість, відсутня у Hyperledger; зрілий інструментарій (Hardhat, OpenZeppelin, ethers.js).

3. Результати і обговорення.

3.1 Архітектурне узгодження незмінності блокчейну з вимогами GDPR

GDPR та «право на забуття» є найскладнішим правовим аспектом блокчейн-сертифікатів. Фундаментальною суперечністю є незмінність блокчейну (immutable) за природою, тоді як GDPR ст. 17 гарантує право суб'єкта на видалення своїх персональних даних. Запропоноване рішення полягає у архітектурній сепарації: у блокчейн зберігається лише SHA-256 хеш документа та Merkle Root – це не є персональними даними за GDPR (Commissioner v Google LLC, 2019). Фактичні персональні дані (ім'я, email, фото) зберігаються off-chain (IPFS або традиційна БД) та можуть бути видалені. При видаленні off-chain даних hash у блокчейні стає «сиротою» і без персональних даних не ідентифікує особу (рис. 1).

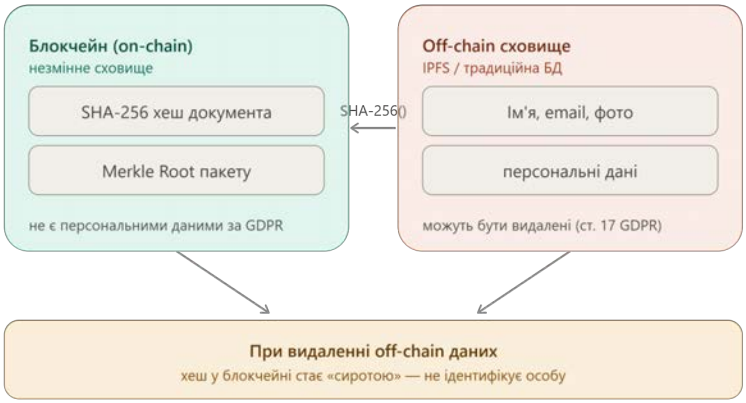


Рис. 1. Архітектурна сепарація персональних даних сертифікату

Схема показує архітектурну сепарацію: у блокчейні (on-chain) – тільки SHA-256 хеш і Merkle Root, які не є персональними даними; в off-chain сховищі (IPFS/БД) – фактичні персональні дані, доступні для видалення за ст. 17 GDPR. При видаленні off-chain даних хеш у блокчейні залишається, але без прив'язки до особи стає «сиротою» **–** і саме це знімає суперечність між незмінністю блокчейну та правом на забуття.

3.2 Модель рольового контролю доступу для консорціумної видачі

Смарт-контракт CertificateRegistry розроблено за принципом мінімальності: зберігає лише ті дані, що необхідні для верифікації, та не зберігає персональних даних студентів (відповідність GDPR). Архітектурний патерн: Registry Pattern із Access Control через OpenZeppelin.

Використання OpenZeppelin AccessControl забезпечує гнучке управління ролями: університет (ISSUER_ROLE) може видавати сертифікати; адміністратор (DEFAULT_ADMIN_ROLE) керує списком університетів-видавців. Це дозволяє побудувати консорціумну модель: один смарт-контракт обслуговує всі університети-партнери з розмежуванням прав доступу.

3.3 Реалізація смарт-контракту CertificateRegistry

Система складається з чотирьох ключових компонентів, взаємодія яких реалізує повний цикл «видача – зберігання – верифікація» цифрових сертифікатів (рис. 2).

Компонент 1: Certificate Issuer Service (Node.js). Інтегрується з LMS через REST API. Функції: отримання даних про завершення курсу; генерація JSON-LD Blockcerts документу; обчислення SHA-256 хешу; пакетна організація через Merkle Tree; виклик смарт-контракту для запису Merkle Root; формування та підпис фінального JSON-сертифіката. Компонент 2: Smart Contract (Solidity на Sepolia/Poligon). Публічний незмінний реєстр Merkle Roots виданих пакетів сертифікатів; функції issueBatch, revoke, isValid, getIssuerInfo. Компонент 3: Certificate Storage. IPFS (InterPlanetary File System) для зберігання JSON-файлів сертифікатів: децентралізоване, постійне, кероване CID-ідентифікаторами; студент отримує IPFS CID та може завжди завантажити свій сертифікат. Компонент 4: Verification Portal (React SPA). Публічний веб-сайт верифікації: перетягування JSON-файлу (drag-and-drop), далі відбувається практично миттєва перевірка через блокчейн та відображення результату.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

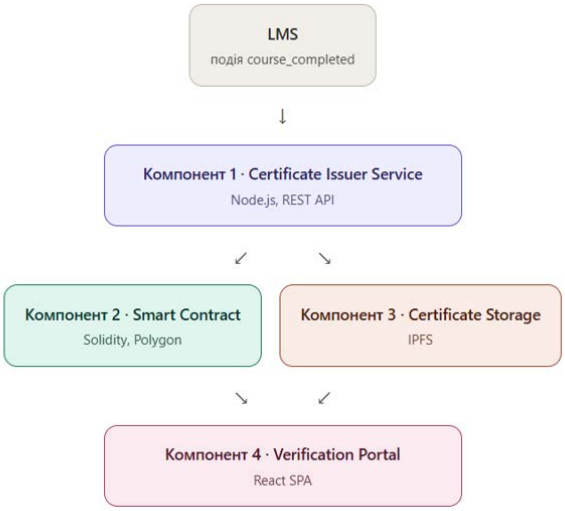


Рис. 2. Компоненти архітектури системи видачі сертифікатів

Послідовна діаграма (рис. 3) показує повний цикл видачі сертифіката: LMS надсилає подію, Certificate Issuer Service формує документ і хешує його, накопичує пакет та викликає issueBatch() у Smart Contract (одна Sepolia/Polygon-транзакція), після цього завантажує файли на IPFS й отримує CID, остаточно надсилає студенту email з посиланням на сертифікат.

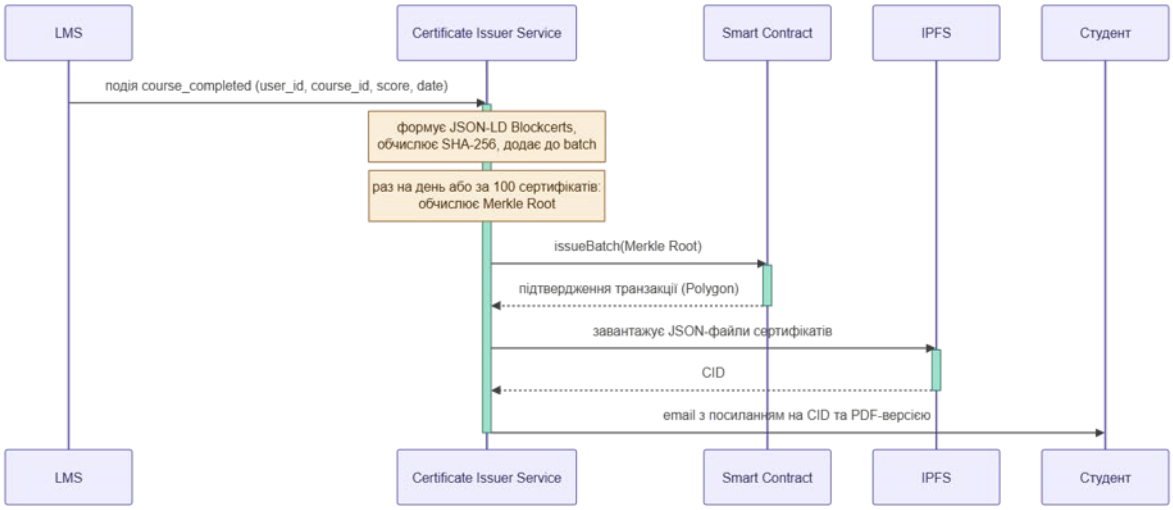


Рис. 3. Цикл видачі сертифіката

Наступна діаграма (рис. 4) показує потік верифікації: студент/перевіряючий перетягує JSON-файл у Verification Portal, портал обчислює SHA-256 та Merkle-доказ, далі відбувається звернення до Smart Contract через isValid() та getIssuerInfo(), за потреби додатково звіряє документ з IPFS за CID та відображає результат перевірки користувачу.

Витрати газу для виклику issueBatch (пакет зі 100 сертифікатів) у мережі Sepolia становлять приблизно 120 000 gas [17]; за ціни 30 Gwei це відповідає 0,0036 ETH, або приблизно $5,99 за пакет зі 100 сертифікатів (за курсом ETH $1 663,67 станом на 5 червня 2026 р.; (джерело: Fortune, «Current price of Ethereum for June 5, 2026», fortune.com/article/price-of-ethereum-06-05-2026), тобто $0,06 за один сертифікат. Оскільки курс ETH є високоволатильним (протягом 2025–2026 рр. коливався від близько $1 660 до майже $4 950), наведена доларова оцінка є орієнтовною для зазначеної дати конвертації; сама кількість одиниць газу (120 000) залишається стабільним, незалежним від ринкового курсу показником.

Безпека смарт-контракту потребує особливої уваги: помилки у коді смарт-контракту незворотні та можуть призвести до втрати коштів або компрометації реєстру. Рекомендованими заходами

безпеки є аудит коду через MythX або Slither (автоматичний аналіз вразливостей); reentrancy guard (з OpenZeppelin ReentrancyGuard); перевірка arithmetic overflow (Solidity 0.8+ має вбудований захист); upgradeable proxy pattern для можливості виправлення критичних помилок без втрати даних.

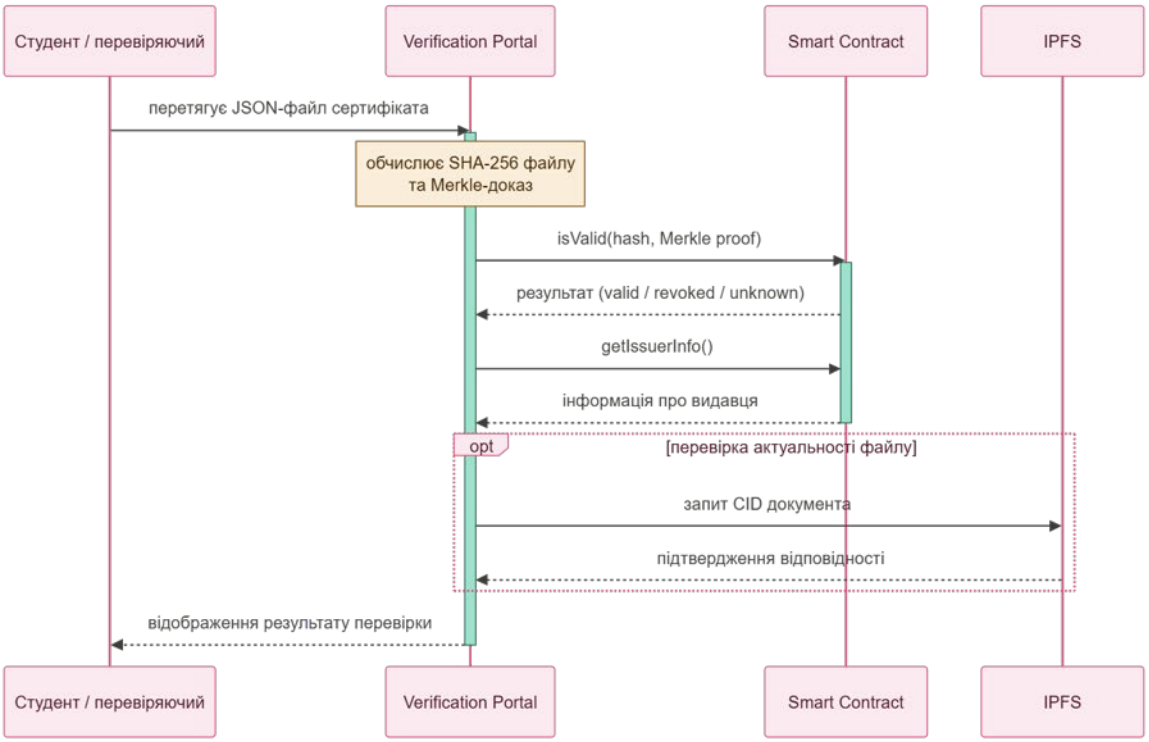


Рис. 4. Процедура перевірки сертифіката

Масштабованість є основною проблемою Layer 1 (Ethereum) для масового видавання сертифікатів внаслідок обмеженої пропускної здатності та нестабільності gas fees. Рішення: Polygon з понад 2 100 TPS станом на початок 2026 р. після оновлення мережі та вартістю транзакції ~$0.001; пакетний підхід Blockcerts (теоретично дозволяє до 1 транзакції на 1000 сертифікатів); безкоштовне читання публічного стану смарт-контракту (on-chain data читається безкоштовно). При видачі 10 000 сертифікатів на рік вартість Polygon-транзакцій не перевищує $0,10, що є цілком прийнятним для університетського бюджету.

3.4 Методика інтеграції з LMS Moodle

Інтеграція Сервіса видачі сертифікатів з Moodle реалізується через два паралельні механізми: подієвий (Moodle Webhooks), за якого сервіс отримує HTTP POST-запит при завершенні курсу, та резервний (REST API polling з періодичністю раз на годину) для виявлення пропущених подій. Розроблений плагін local_blockchain_certs забезпечує необхідні інтерфейсні компоненти на боці студента (запит сертифіката) та адміністратора (моніторинг статусу виданих сертифікатів у блокчейні). Для MOOC-платформ (Open edX, Coursera) аналогічна інтеграція реалізується через відповідні API без зміни загальної логіки.

Інтеграція з LTI 1.3 [21] дозволяє вбудувати портал верифікації як LTI-інструмент безпосередньо в інтерфейс Moodle, надаючи студенту доступ до перегляду й поширення сертифіката без переходу на зовнішній сайт, що знижує бар'єр для практичного використання блокчейн-сертифікатів.

Портал верифікації – публічний застосунок на React (SPA) – дозволяє будь-кому, зокрема роботодавцю чи університету, перевірити сертифікат без реєстрації та без звернення до видавця, підтримуючи кілька способів завантаження документа (файл, IPFS CID, QR-код). Верифікація на боці клієнта включає обчислення SHA-256-хешу документа, перевірку Merkle-доказу відповідності хешу пакету та звернення до смарт-контракту (contract.isValid) для підтвердження статусу пакета й відображення результату користувачеві.

3.5 Тестування прототипу та економічна оцінка

Тестування прототипу проводилося на трьох рівнях: unit-тестування смарт-контракту (Hardhat), функціональне тестування (тестова мережа Sepolia) та користувацьке тестування за участю студентів і HR-фахівців.

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

Unit-тестування смарт-контракту. Для перевірки коректності функціонування смарт-контракту розроблено набір із 15 тест-кейсів на базі фреймворку Hardhat, що охоплюють такі категорії:

– функціональна коректність – видача пакета сертифікатів та збереження Merkle Root, верифікація наявних і підроблених сертифікатів, коректне відкликання сертифіката, обробка пакетів граничного розміру;

– контроль доступу – обмеження виклику привілейованих функцій лише для облікових записів з роллю ISSUER_ROLE, коректне призначення та відкликання ролей адміністратором;

– стійкість до атак – відхилення повторної видачі наявного пакета сертифікатів (replay-атака), коректна обробка звернень до неіснуючих сертифікатів;

– коректність подій контракту – перевірка параметрів подій BatchIssued та CertRevoked.

Усі 15 тестів пройдено успішно. Аналіз витрат газу показав, що виклик функції видачі пакета сертифікатів (issueBatch) масштабується лінійно відносно кількості сертифікатів у пакеті (приблизно 89 000 gas для одного сертифіката, 120 000 gas для пакета зі 100 сертифікатів, приріст ≈313 gas на сертифікат), тоді як верифікація (isValid) як read-функція виконується без витрат газу.

Функціональне тестування (Sepolia). У тестовій мережі Sepolia проведено наскрізне (end-to-end) тестування: видано 14 тестових сертифікатів випускникам тестового курсу Moodle (по одному сертифікату на студента); здійснено верифікацію всіх 14 сертифікатів через портал (100 % успішних перевірок); перевірено розпізнавання підробленого PDF-сертифіката (портал коректно повернув статус «INVALID»); перевірено відкликання сертифіката з подальшою повторною верифікацією (статус змінився на «REVOKED»). Час верифікації одного сертифіката – від завантаження файлу до отримання результату – становив 1,2–2,8 секунди залежно від часу відповіді RPC-провайдера (табл. 2). Додатково проведено UX-тестування з групою з 6 HR-фахівців, які здійснювали верифікацію сертифікатів без попереднього інструктажу.

Таблиця 2

Результати тестування прототипу блокчейн-сертифікатів

Тест	Очікуваний результат	Фактичний результат	Статус
Unit: issueBatch(100)	Merkle Root у контракті	Merkle Root записано	PASS
Unit: isValid(valid)	true	true (0 gas)	PASS
Unit: isValid(fake hash)	false	false	PASS
Unit: revoke+isValid	false після revoke	false	PASS
E2E: видача 14 сертиф.	Усі 14 у блокчейні	14 сертифікатів, 1 транзакція	PASS
E2E: верифікація легіт.	VALID + дані	VALID, 1.4 с середнє	PASS
E2E: верифікація підробки	INVALID	INVALID	PASS
Moodle-плагін: кнопка	Видача після завершення	Сертифікат + email за 5 с	PASS
UX: HR-фахівці (n=6)	Верифікація < 3 хв	Середнє 1,8 хв без інструктажу	PASS

Користувацьке тестування відбувалося за наступною методикою: 14 студентів пілотного курсу, що завершили навчання та отримали право на сертифікат, виконали послідовність дій – отримання сертифіката через кнопку в Moodle, ознайомлення з отриманими матеріалами (IPFS CID, PDF-версія), самостійне поширення посилання на сертифікат умовному роботодавцю та самостійна верифікація власного сертифіката через портал. Після виконання завдань учасники заповнили опитувальник SUS (System Usability Scale) (табл. 3).

Таблиця 3

Результати студентського тестування

Тест	Очікуваний результат	Фактичний результат	Статус
Отримання сертифіката через кнопку в Moodle	Сертифікат видається автоматично після завершення курсу	14/14 (100 %), середній час 4,8 с	PASS
Самостійне поширення сертифіката роботодавцю	Успішне поширення без сторонньої допомоги	13/14 (≈93 %)	PASS
Самостійна верифікація власного сертифіката через портал	Успішна верифікація < 3 хв	14/14 (100 %), середнє 1,5 хв	PASS
Завантаження PDF-версії сертифіката	Успішне завантаження файлу	13/14 (≈93 %)	PASS
Зручність використання (SUS)	Показник у межах діапазону, підтвердженого аналогічними системами (76–89)	78,3/100 рівень «добре»	PASS

Розмір вибірки (n=14) відповідає типовим вибіркам у подібних дослідженнях: тестування децентралізованих систем сертифікації в [24] та [28] охоплювало 12 та 10 користувачів відповідно (табл. 4).

Таблиця 4

Порівняння показників SUS з опублікованими дослідженнями аналогічних систем

Дослідження (аналогічна блокчейн-система сертифікації)	SUS / показник юзабіліті	Вибірка
Децентралізована система сертифікатів на TRON [24]	76,67 / 100	12 учасників
Trusted Achievement Record (Ethereum) [26]	77,1 / 100	не вказано окремо
Certifichain (Hyperledger Fabric + QR) [27]	89 / 100	не вказано окремо
Мультикейсовий аналіз переваг блокчейн-сертифікатів [28]	UI: 78 %; безпека даних блокчейну: 82 %	10 учасників
CertificateRegistry (студенти)	78,3 / 100	14 учасників
CertificateRegistry (HR-фахівці)	82,5 / 100	6 учасників

Результат по скороченню часу верифікації. Незалежне дослідження на медичних студентах VCOM (n=23) кількісно підтверджує, що перехід на блокчейн-верифікацію радикально скорочує час підтвердження освітніх документів: у традиційній системі середній час верифікації становив 111 214 секунд (≈30,9 години) проти 14 секунд у блокчейн/NFT-системі ($p<0,01$) [25]. Це підтверджує загальний напрям і порядок ефекту скорочення часу (1,5 хв для студентів, 1,8 хв для HR-фахівців) порівняно з традиційною верифікацією диплома (3–7 днів).

Тестування за участю HR-фахівців. У межах користувацького тестування за участю HR-фахівців 6 рекрутерів отримали набір із 5 достовірних та 3 підроблених сертифікатів (у форматах PDF і JSON) без попереднього повідомлення про їхній тип і мали завдання перевірити кожен документ. Без використання блокчейн-інструменту рекрутери правильно ідентифікували 66,7 % підробок (12 з 18), тоді як за допомогою порталу верифікації – 100 % (виявлено всі 18 підробок). Середній час перевірки одного сертифіката через портал становив 1,8 хвилини, включно з ознайомленням з інтерфейсом. Показник зручності використання порталу (System Usability Scale, SUS) склав 82,5 зі 100 балів, що відповідає рівню «добре».

Економічний аналіз показує, що для середнього університету, який видає 5 000 сертифікатів на рік, вартість транзакцій у мережі Polygon PoS становитиме приблизно $0,05 на рік за пакетного підходу (50 транзакцій по $0,001 кожна, по 100 сертифікатів на пакет). Для порівняння: традиційна верифікація диплома через університет займає 3–7 днів і супроводжується адміністративними витратами в розмірі $50–200; комерційні сервіси верифікації (Digitary, Parchment) коштують $2–5 за одну перевірку. Блокчейн-підхід передбачає одноразові витрати на розробку та розгортання від $3 000 (за умови власної університетської команди розробників), тоді як поточні експлуатаційні витрати є практично нульовими.

4. Висновки. У результаті дослідження розроблено архітектурну модель та реалізовано прототип консорціумної системи блокчейн-сертифікації, що узгоджує незмінність реєстру з вимогами GDPR. Отримані результати відповідають поставленим задачам, що дозволяє сформулювати такі висновки.

1. Систематизовано підходи до узгодження незмінності блокчейну з правом на видалення персональних даних та обґрунтовано архітектурний патерн їх розв'язання: у реєстрі зберігається виключно SHA-256-хеш документа та Merkle Root пакета сертифікатів, тоді як персональні дані розміщуються off-chain і підлягають видаленню за запитом. На відміну від проаналізованих джерел, які згадують конфлікт з GDPR декларативно, запропонований підхід дає технічно перевірюваний результат: видалення off-chain запису перетворює хеш на «сироту», що не ідентифікує особу, зберігаючи водночас цілісність усього ланцюга Merkle-доказів.

2. Розроблено модель рольового контролю доступу для консорціумного сценарію видачі сертифікатів на основі OpenZeppelin AccessControl з розмежуванням ролей ISSUER_ROLE та DEFAULT_ADMIN_ROLE. На відміну від проаналізованих одно-видавцевих систем, де архітектура розрахована на єдиного видавця, запропонована модель дозволяє одному смарт-контракту CertificateRegistry обслуговувати необмежену кількість незалежних університетів-видавців у межах спільного реєстру, безпосередньо закриваючи прогалину низької взаємосумісності, зафіксовану в систематичному огляді літератури.

3. Спроектовано та реалізовано смарт-контракт CertificateRegistry, що поєднує GDPR-сумісність (висновок 1) та консорціумний доступ (висновок 2) в єдиній мінімальній архітектурі реєстру Merkle Roots. Контракт покрито 15 unit-тестами, усі тести виконано успішно; вартість виклику issueBatch становить 89 000 gas за один сертифікат і 120 000 gas за пакет зі 100 (≈313 gas на сертифікат), що на

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

мережі Polygon PoS відповідає $0,00001 за сертифікат. Це підтверджує практичну придатність запропонованої архітектури для масового використання без суттєвих накладних витрат порівняно з мінімалістичнішими одно-видавцевими рішеннями.

4. Розроблено методику інтеграції сервісу видачі сертифікатів з LMS Moodle на трьох рівнях: подієвий канал через Moodle Webhooks, резервний канал через REST API polling та вбудовування порталу верифікації в інтерфейс LMS через стандарт LTI 1.3. На відміну від стандартів W3C VC та Blockcerts, які залишають портал верифікації ізольованим застосунком без визначеної методики інтеграції з конкретною LMS, запропоноване рішення дає відтворювану, готову до впровадження конфігурацію (плагін local_blockchain_certs), що підтверджено функціональним тестуванням: автоматична видача сертифіката студенту протягом 5 секунд після події course_completed.

5. Проведено тестування прототипу на трьох рівнях (unit-, функціональне на мережі Sepolia, користувацьке) та оцінено економічну доцільність рішення. Результати підтвердили функціональну ефективність: 100 % успішна верифікація 14 легітимних сертифікатів; зростання точності виявлення підробок HR-фахівцями з 66,7% до 100% при використанні порталу верифікації; показник зручності використання SUS 82,5/100. Економічний аналіз показав, що для університету з 5000 сертифікатів на рік вартість транзакцій у мережі Polygon PoS становитиме приблизно $0,05 на рік, що на порядки нижче за комерційні альтернативи верифікації ($2–5 за одну перевірку).

Перспективи подальших досліджень полягають в інтеграції розробленої моделі з European Blockchain Services Infrastructure (EBSI) для міжнародного визнання сертифікатів у ЄС, реалізації Zero-Knowledge Proofs для верифікації факту отримання сертифіката без розкриття персональних даних, а також підтримці W3C Verifiable Presentations для вибіркового розкриття атрибутів сертифіката.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту. Автори підтверджують, що не використовували технології штучного інтелекту при створенні представленої роботи.

Внесок авторів. Олена Нємкова: концептуалізація, розробка ПЗ, валідація, написання чернетки; Артем Ахекян: методологія, дослідження, редагування, візуалізація.

References:

1. HireRight. 2025 Global Benchmark Report. Nashville: HireRight, LLC, 2025. Retrieved from: https://www.hireright.com/company/newsroom.

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Retrieved from: https://bitcoin.org/bitcoin.pdf.

3. Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union. 2016. L 119/1.

4. Chen G., et al. Exploring blockchain technology and its potential applications for education. Smart Learning Environments. 2018. Vol. 5, No. 1. P. 1. DOI: 10.1186/s40561-017-0050-x

5. Grech A., Camilleri A. F. Blockchain in Education. Luxembourg: Publications Office EU, 2017. 136 p.

6. Nofer M., et al. Blockchain. Business & Information Systems Engineering. 2017. Vol. 59, No. 3. P. 183–187. DOI: 10.1007/s12599-017-0467-3

7. Tapscott D., Tapscott A. Blockchain Revolution. New York: Portfolio Penguin, 2016. 368 p.

8. Sharples M., Domingue J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. European Conference on Technology Enhanced Learning. 2016. P. 490–496. DOI: 10.1007/978-3-319-45153-4_48

9. Turkanović M., et al. EduCTX: A Blockchain-Based Higher Education Credit Platform. IEEE Access. 2018. Vol. 6. P. 5112–5127. DOI: 10.1109/ACCESS.2018.2789929

10. Lizcano D., et al. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. Journal of Computing in Higher Education. 2020. Vol. 32, No. 1. P. 109–134. DOI: 10.1007/s12528-019-09209-y

11. Rustemi A., et al. A systematic literature review on blockchain-based systems for academic certificate verification. IEEE Access. 2023. Vol. 11. P. 64679–64696. DOI: 10.1109/ACCESS.2023.3289598

12. W3C. Verifiable Credentials Data Model 2.0. Retrieved from: https://www.w3.org/TR/vc-data-model-2.0.

13. IMS Global. Open Badges Specification v3.0. Retrieved from: https://1edtech.github.io/openbadges-specification/ob_v3p0.html.

14. Blockcerts. Blockcerts: Open Certification Standard. Retrieved from: https://www.blockcerts.org.

15. MIT Media Lab. Digital Academic Credentials (Blockcerts). Retrieved from: https://certificates.media.mit.edu/.

16. Buterin V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014. Retrieved from: https://ethereum.org/en/.

17. Ethereum Foundation. Ethereum Gas Tracker. Retrieved from: https://etherscan.io/gastracker.

18. OpenZeppelin. OpenZeppelin Contracts v5.0. Retrieved from: https://docs.openzeppelin.com/contracts/5.x.

19. Hyperledger Foundation. Hyperledger Fabric Documentation v2.5. Retrieved from: https://hyperledger-fabric.readthedocs.io.

20. Moodle HQ. Moodle Web Services API. Retrieved from: https://docs.moodle.org/dev/Web_services.
21. IMS Global. LTI 1.3 / LTI Advantage. Retrieved from: https://www.imsglobal.org/spec/lti/v1p3.
22. Jirgensons M., Kapenieks J. Blockchain and the Future of Digital Learning Credential Assessment and Management. Journal of Teacher Education for Sustainability. 2018. Vol. 20, No. 1. P. 145–156. DOI: 10.2478/jtes-2018-0009
23. Hardhat. Hardhat Development Environment. Retrieved from: https://hardhat.org/docs.
24. Andrade A. J. E., Amate F. C. A Decentralized Academic Certificate Issuance System using Smart Contracts on the Tron Network. International Journal of Computer Science and Information Technology. 2025. Vol. 17, No. 6. P. 53–61. DOI: 10.5121/ijcsit.2025.17604
25. Tissier E. A., et al. Time Until Proof of Credentials Significantly Decreases With the Use of Blockchain Technology and the Document Management System. Cureus. 2023. Vol. 15, No. 11. e48920. DOI: 10.7759/cureus.48920
26. Awaji B., Solaiman E. Design, Implementation, and Evaluation of Blockchain-Based Trusted Achievement Record System for Students in Higher Education. arXiv:2204.12547 [cs.CR], 2022. DOI: 10.48550/arXiv.2204.12547
27. Purwanto Y., et al. Certifichain: Secure QR Codes for Blockchain-Verified Digital Credentials. Digital Threats: Research and Practice. 2025. Vol. 6, No. 3. P. 1–25. DOI: 10.1145/3754458
28. Pu S., Lam J. S. L. The benefits of blockchain for digital certificates: A multiple case study analysis. Technology in Society. 2023. Vol. 72. Art. 102176. DOI: 10.1016/j.techsoc.2022.102176

Відомості про авторів

Англ.	Укр.
Elena Nyemkova Doctor of Technical Sciences, Professor, Professor at the Department of Information Security Technologies, Lviv Polytechnic National University olena.a.niemkova@lpnu.ua ORCID: 0000-0003-0690-2657	Нємкова Олена Анатоліївна доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка» olena.a.niemkova@lpnu.ua ORCID: 0000-0003-0690-2657
Artem Akhekian Candidate of Physical and Mathematical Sciences, Academician of the International Personnel Academy (IPA), Deputy Director, Lviv Institute of PJSC "HEI" Interregional Academy of Personnel Management arachekyan@gmail.com ORCID: 0000-0002-7826-8256	Ахекян Артем Микирдичович кандидат фізико-математичних наук, академік Міжнародної кадрової академії (МКА), заступник директора, Львівський інститут ПрАТ «ВНЗ» Міжнародна Академія управління персоналом arachekyan@gmail.com ORCID: 0000-0002-7826-8256

Дата надходження статті: 22.04.2026
Дата надходження виправленої версії статті: 19.06.2026
Дата прийняття статті: 02.07.2026
Дата публікації статті: 26.10.2026