© Opirskyy I., Balatska V., Poberezhnyk V. Modern possibilities of use blockchain technology in the education system// Ukrainian Scientific Journal of Information Security, 2023, vol. 29, issue 3, pp. 138-146. ©

ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ/ PRIVACY & PROTECTION FROM IDENTITY THEFT

DOI: 10.18372/2225-5036.29.18073

СУЧАСНІ МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СИСТЕМІ ОСВІТИ

Іван Опірський, Валерія Балацька, Василь Побережник

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., проф.
Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: завідувач кафедри захисту інформації з 2023 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання.
Публікації: : більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

БАЛАЦЬКА Валерія Сергіївна, аспірант.
Рік та місце народження: 1996 рік, м. Луцьк, Волинська обл., Україна.
Освіта: Львівський державний університет безпеки життєдіяльності, 2019 рік.
Посада: аспірант кафедри захисту інформації, з 2022 року.
Наукові інтереси: комп'ютерні мережі, операційні системи, захист інформації, комплексні системи захисту інформації, захист персональних даних.
Публікації: більше 20 публікацій серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: valeriia.s.balatska@lpnu.ua.
Orcid ID: 0000-0002-6262-6792.

ПОБЕРЕЖНИК Василь Олегович, аспірант.
Рік та місце народження: 1995 рік, м. Львів, Львівська обл., Україна.
Освіта: Національний університет «Львівська політехніка», 2018 рік.
Посада: аспірант кафедри захисту інформації, з 2022 року.
Наукові інтереси: технології блокчейн, захист приватності, децентралізовані системи.
Публікації: 5 публікацій, серед яких наукові статті, монографія, тези та матеріали доповідей на конференціях.
E-mail: vasyl.poberezhnyk@gmail.com.
Orcid ID: 0000-0002-7523-2557.

Анотація*. Технологія блокчейн традиційно привертає увагу за рахунок потенціалу революціонізувати різні галузі – передусім фінанси та управління ланцюжками постачання. Про освіту в даному контексті говорять рідко, однак і в ньому є, що трансформувати, наприклад, сертифікацію, видачу дипломів, атестатів. При цьому блокчейн у сертифікації – це не просто підтвердження знань та академічної чистоти, а про новий підхід через створення системи зберігання та розподілу інформації про результати навчання. У цій статті досліджується потенційне застосування технології блокчейн в освітньому секторі, з акцентом на унікальні випадки використання, пов'язані з курсами, платіжками, іспитами та кваліфікаціями. Смарт-контракти -*

це самодостатні контракти із заздалегідь визначеними умовами. Ці контракти працюють у мережі блокчейн, усуваючи потребу в посередниках і забезпечуючи довіру, прозорість та автоматизацію. В освітньому секторі смарт-контракти можуть впорядкувати адміністративні процеси, підвищити безпеку та забезпечити послідовний облік досягнень. Вони розширюють можливості як учнів, так і навчальних закладів, надаючи децентралізовану платформу для навчання, оцінювання та сертифікації. Метою статті є дослідження можливостей та перспективи використання технології блокчейн та смарт-контрактів у науці та освіті.

***Ключові слова**: блокчейн, смарт-контракт, освіта, децентралізована система, захист персональних даних.*

Постановка проблеми

Основною проблемою з якою стикається будь-яка сфера діяльності в Україні, зокрема, освітня, це ряд таких проблем як: зберігання паперових версій документів в архівах навчальних закладів, що супроводжується ризиком їхньої підробки та втрати. Також, паперовий носій може згоріти, загубитися, до нього можуть внести зміни або просто зіпсувати. Наступною не менш важливою проблемою є введення історії успішності здобувачів на паперових носіях, що дає можливість не лише внести зміни до документа, а й створює додаткове бюрократичне навантаження на викладацький склад, що знижує якість навчання.

Наступним великим мінусом освітньої сфери діяльності є відсутність єдиного ресурсу, де можна було б знайти цікавий курс у будь-якій точці світу, адже сьогодні ми легко можемо поїхати куди завгодно, але швидко знайти потрібний курс буває вкрай складно. Також, відсутність довіри у роботодавців до академічних даних, що надаються, оскільки підтвердити кваліфікацію часом дуже складно, роботодавцям доводиться вигадувати різні тестові завдання при прийомі на роботу, все це значно знижує цінність освіти. Складність пошуку фахівців, які мають специфічні навички: немає єдиного алгоритму, тому рекрутерам дуже складно навіть просто звузити коло пошуку. Вирішення вищезазначених проблем полегшить організацію навчального процесу для всіх учасників, а його результати не викликатимуть сумнівів ні у роботодавців, ні у приймальній комісії. Щоб досягти цього, необхідне комплексне рішення та впровадження у сферу освіти сучасних технологій.

Блокчейн – це відносно нова парадигма управління цифровими даними та навчання. Багато дослідників вважають, що це новий мегатренд цифрового світу [1]. Без сумніву, це відіграє важливу роль у навчальному процесі, де це відбувається на кількох рівнях. Наприклад, він знаходить застосування в організації освіти, шляхом впровадження децентралізованих платформ, що містять оцінки, документи чи дипломи випускників, або автентифікації та безпеки процесів, пов'язаних із перевіркою знань, таких як іспити. Крім того, це цінні знання, яким можна і навіть потрібно навчати.

Блокчейн функціонує на інтерфейсі з іншими технологіями, такими як штучний інтелект, IoT, Big Data. Ці рішення повільно проникають у практику викладання, наприклад, технічно підтримуючи оцінювання, контроль або профілювання. Через це ці методи, незважаючи на їхні безсумнівні переваги, здаються культурно інвазивними та можуть викликати серйозні етичні питання.

Аналіз останніх досліджень і публікацій

Сьогоднішні студенти здобувають освіту різними шляхами, не тільки у традиційних лекційних залах університетів. В даний час існують різні онлайн-курси, семінари та конференції, місця для спільного навчання та навчальні платформи.

Традиційна централізована модель сучасного навчання не є єдиною. Технологія Blockchain дозволяє децентралізувати та «Дезінтермедіювати» вищу освіту [3]. Онлайн-навчання може здійснюватися через блокчейн, що дозволить легко перевіряти та передавати навички та повноваження [4, 5].

Зберігання даних про освіту (Storing Permanent Records). Якщо дані про освіту постійно зберігатимуться у блокчейні, такі документи як дипломи, атестати та сертифікати про освіту, наукового ступеня, можуть бути захищені та перевірені незалежно від того, чи має користувач доступ до системи записів навчального закладу. Навіть якщо установи, які видавали сертифікати, мали закритися, або якщо вся система освіти впала (як, наприклад, сталося в Сирії), ці сертифікати все ще можна перевірити за записами, що зберігаються в блокчейні [6, 7].

Європейська комісія вважає, що після того, як установи випустять диплом, атестат, сертифікат, їм не потрібно витрачати додаткові ресурси на підтвердження дійсності цього сертифіката третім сторонам, оскільки, вони зможуть самі перевіряти сертифікати безпосередньо у блокчейн [4].

Наступним кроком є перевірка особистості та інформаційна безпека (Identity Verification & Information Security). Використовуючи блокчейн, студенти та інші здобувачі можуть ідентифікувати себе онлайн, зберігаючи контроль над зберіганням та керуванням своїми особистими даними. В даний час студенти повинні регулярно ідентифікувати себе у своїй навчальній установі. У результаті десятки чи сотні людей можуть мати доступ до особистої інформації студента. Забезпечення безпеки цих даних вимагає управління правами доступу та забезпечення того, щоб система доступу до особистої інформації була також безпечна та захищена від злому.

За допомогою блокчейн лише деякі обрані, а саме сторони, відповідальні за перевірку особи здобувача, а також сам студент, можуть мати доступом до даних. Це означає, що навчальним установам більше не потрібно керувати складними системами для отримання прав доступу, а потрібно тільки захищати

мережу, де проводиться первісна перевірка. Це дозволить заощадити значні ресурси, витрачені на захист мережі від злому даних, навчання персоналу, захисту даних та управління правами доступу [8].

Блокчейн дозволяє особистим даним бути просто особистими. Студенти отримують контроль та право володіння всіма своїми даними про освіту, включаючи акредитацію та портфоліо робіт, у безпечному місці, доступному для всіх, кому необхідно це перевірити та зберігається протягом усього життя [9].

Мета та постановка завдання

Традиційна передача та зберігання знань, насамперед через школи та університети, є освяченим часом, цінним і важливим визначальним фактором, який представляє інтелектуальний розвиток, прогрес і покращення повсякденного життя. Однак, з іншого боку, щоб ефективно функціонувати в сучасному, динамічному та конвергентному середовищі, освітні установи повинні характеризуватися відкритістю та високим динамізмом у засвоєнні нових ідей та інновацій, особливо у сфері ІКТ [2].

Виклад основного матеріалу дослідження

Блокчейн — це вічний цифровий розподілений журнал економічних транзакцій, який може бути запрограмований для запису не лише фінансових операцій, а й практично всього цінного [10].

Дві важливі властивості блокчейн:

1. Прозорість — дані впроваджені в мережу цілком і вони, за визначенням, є публічними.
2. Він не може бути зруйнований – зміна будь-якої одиниці інформації в блокчейн потребує використання гігантської обчислювальної потужності, щоб підмінити інформацію по всій мережі.

Саме для захисту та швидкої валідації інформації використовується хешування - перетворення масиву вхідних даних довільної довжини у (вихідний) бітовий рядок встановленої довжини, що виконується певним алгоритмом.

Процес укладання будь-якої угоди – це насамперед складання контракту, в якому прописані всі умови, права та зобов'язання сторін, що беруть участь. Однак у більшій частині договорів присутні не тільки сторони, які укладають угоду, а й посередники – банки, нотаріуси, реєстратори, регулятори. Завдяки активному розвитку технології блокових ланцюгів (блокчейн) ця потреба залишається в минулому – на зміну звичайним контрактам прийшли так звані «розумні» контракти, з англійської – смарт-контракт.

Технологія смарт-контрактів сама по собі також є перспективною технологією для багатьох галузей, у тому числі для освіти.

Смарт-контракт комп'ютерний алгоритм, призначений для укладання та підтримки комерційних контрактів у технології блокчейн [11].

Такі угоди можуть укладатися між двома людьми, іншими словами, peer-to-peer (P2P), людиною та організацією (P2O) або людиною та машиною (P2M).

Смарт-контракти дозволяють автоматизувати платежі та переказ валюти або інших активів як погоджені умови. Як тільки буде виконано задану в розумному контексті умову (наприклад, продаж товарів «1» на біржі «2»), договір виконується автоматично та активи (наприклад, кошти, цифрова валюта, право власності, дані) обмінюються між сторонами. Потім транзакція реплікується та перевіряється на блоковому ланцюжку.

Смарт-контракти дозволяють обміняти актив, якщо треті сторони не знають про передачу. Це відкриває можливість дезінтегрувати всю правову систему та створити нову форму віртуальних угод. Насправді, будучи фрагментами коду, які автоматично виконують дії, коли дотримуються заданих умов, розумні контракти поки що не можуть розглядатися як звичайні контракти з юридичної точки зору. Проте вони можуть використовуватись як доказ вирішення того чи іншого завдання та численні галузі вивчають потенційні можливості застосування таких контрактів.

Для створення смарт-контракту потрібні наступні компоненти:

- предмет договору – програма повинна мати доступ до товарів чи послуг з приводу яких укладається контракт та мати можливість автоматично дати або закрити до них доступ;
- цифрові підписи – всі учасники ініціюють угоду, підписуючи договір своїми секретними ключами;
- умови договору – умови смарт-контракту у формі точної послідовності операцій, які мають підписати усі учасники;
- учасники договору – описані вище моделі між двома людьми (P2P), людиною та організацією (P2O) або людиною та машиною (P2M);
- децентралізована платформа – смарт-контракт записується в блокчейн цієї платформи і розподілено зберігається на її вузлах.

У блокчейн присутні вищеперелічені компоненти. Питаннями захисту та підтвердження дійсності сертифікатів, а також системою репутації за допомогою блокчейн займаються особливо в Массачусетському технологічному інституті. Ними було випущено кілька версій програми Blockcerts з відкритим вихідним кодом, що реалізує облік та видачу сертифікатів з можливістю ділитися ними з роботодавцями [12].

Массачусетський технологічний університет у 2018 році надає можливість студентам отримати цифрову версію їхніх дипломів на блокчейн в рамках експериментальної програми, що дозволяє зробити академічні дані безпечними та переносимі.

Впровадження технології блокчейн дозволить стандартизувати документи, що видаються, що в свою чергу може стандартизувати освіту в усьому

світі. Підтверджені знання та навички кандидатів можуть зберігатися в єдиній базі даних, що дозволить вибирати кандидатів з динамічного відбору виходячи з їхнього набору вмінь та необхідних навичок для обраної посади.

Підсумком створення даної бази даних буде наявність відкритого ринку кандидатів із підтвердженими знаннями. А це, у свою чергу, дозволить створити попит на конкретні компетенції та створить тенденції на вивчення певних освітніх програм, у результаті яких і формуються ці компетенції.

Навчальні заклади можуть визначити необхідний профіль кандидатів і розробити відповідні освітні програми та навчальні курси. Як наслідок, можна скоротити розрив між ринком праці та ринком освіти і вирішити проблему швидкої непрактичності навчальних програм, створених під час бурхливого розвитку інформаційних технологій.

Сьогодні як для установ, так і для компаній підготовка та перевірка відповідності сертифікатів, дипломів та атестатів кандидатів необхідним компетенціям є дорогим і трудомістким процесом. Якщо кандидати не відповідають певним вимогам, компанії можуть зазнати збитків у майбутньому.

База даних може врятувати організації від втрат, пов'язаних з перевіркою дійсності дипломів та сертифікатів [13].

Японська компанія Sony, яка побудувала сервіс Sony Global Education Service, з кінця 2017 року використовує технологію блокчейн для видачі сертифікатів. Своїм прикладом вони намагаються показати, що за цією технологією майбутнє у сфері гарантування автентичності знань, отриманих в освіті [14].

Sony Global Education вважає, що персональні дані про успішність студентів є настільки ж цінними, як, наприклад, кредитна історія людини. При використанні технології блокчейн дані можуть бути підписані цифровим підписом і безпечно передані іншим сторонам. Зберігаючи достовірні дані, можна отримати повну історію абітурієнта (наприклад, у вигляді комп'ютерного тесту) на повністю захищеній платформі.

Таким чином, впровадження технології блокчейн в освіті вже знайшло своє застосування, наведено приклад використання ланцюжка мікрокредитів у відносинах між університетами, студентами та роботодавцями (рис. 1).

Звісно, основний наголос на реалізацію можливості безпечного зберігання сертифікатів, атестатів, дипломів та успішності здобувачі, що може вирішити такі завдання:

1. Стандартизація та глобалізація освіти (можлива стандартизація без глобалізації);

2. Наявність достовірного, відкритого та єдиного ринку кандидатів з підтвердженими знаннями;

3. Актуальність освітніх програм, а, отже, скорочення розриву між ринком праці так ринком освіти.

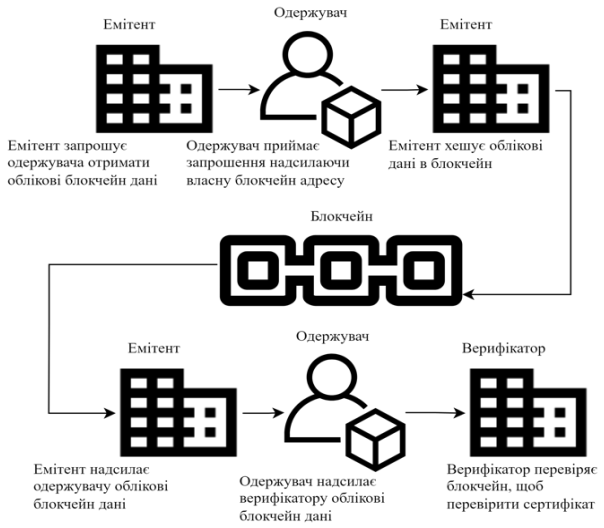

Рис. 1. Ланцюжок мікро-облікових даних

На основі проведеного дослідження виводяться такі сценарії застосування технології блокчейн в освіті:

- ідентифікація студента;
- облік успішності студента;
- оплата за навчання;
- стипендії та заохочення;
- зв'язування кожних нових отриманих оцінок з цілями та знаннями, які у свою чергу, пов'язуються з отриманими раніше цілями та знаннями, на яких вони засновані та рівень яких також було оцінено;
- автоматична видача дипломів, атестатів та сертифікатів при досягненні певного результату;
- підтвердження дійсності дипломів, атестатів та сертифікатів;
- безпечне зберігання та передача інформації;
- проведення тестувань, опитувань та голосувань;
- залучення інвестицій;
- акредитація та контроль за освітньою установою.

У свою чергу, хорошою ідеєю є використання смарт-контрактів для оформлення угоди між абітурієнтами та університетом, де результатом виконання всіх умов, наслідком буде одержання диплома та особливо цифрової його версії на основі блокчейну. Смарт-контракт включає перелік умов, які має виконати абітурієнт для успішного закриття угоди: проходження вступних іспитів до ВНЗ, завершення всіх семестрів, проходження виробничої та переддипломної практики, захист дипломної роботи.

Впровадження смарт-контрактів та технології блокчейн допоможе підвищити статус української освіти у всьому світі.

Управління академічних даних студентів та їх захист

Використання технології блокчейн в системах управління інформаційними системами можна спо-

стерігати незалежно від сфери людської діяльності [15]. Тому закономірно, що дослідження можливостей використання технології для управління навчальними профілями студентів та можливості моніторингу і внесення даних відповідно до їх успішності стало предметом наукового інтересу. Наприклад, запропонована в система управління навчанням на основі блокчейн поєднує технологію блокчейн та смарт-контракти, що дозволяє передати частину адміністративних та викладацьких завдань від персоналу вищих навчальних закладів до самої системи [16].

Такий підхід забезпечує вільний доступ до даних про оцінки учнів та загальний прогрес у навчанні. По-перше, такий підхід дозволяє зберігати інформацію про успішність учнів децентралізовано, що захищає дані від можливості втрати через форс-мажорні обставини.Крім того, використання технології блокчейн підвищує рівень довіри між сторонами, залученими до освітнього процесу, оскільки захищає інформацію від несанкціонованих змін, завдяки характеристикам технології, які гарантують незмінність збереженої інформації та відсутність користувачів зі спеціальними повноваженнями, таких як системні адміністратори. Використання технології смарт-контрактів також виключає або мінімізує людський фактор при оцінюванні результатів навчання.

Хоча необхідність захисту інформації про студентів очевидна, існує критична потреба у створенні децентралізованих систем, оскільки центральна точка вразливості є неприйнятною в сьогоднішніх реаліях. Актуальність такої системи буде лише зростати, оскільки росія серйозно вторглася в Україну, змусивши багато вищих навчальних закладів переїхати з тимчасово окупованих територій на підконтрольну Україні територію. Таким чином, наявність такої системи не лише спростила б процес передачі даних у форс-мажорних ситуаціях, але й мінімізувала б можливість втрати даних про студентів, оскільки децентралізований характер системи гарантує відсутність центральної точки вразливості.

Крім того, такий підхід не тільки забезпечує безпеку даних на стороні ВНЗ, але й відновлює доступ до можна втратити. Відновлення втраченого гаманця не вимагає практично ніяких дій з боку мережі, лише наявність ключової фрази [17]. Іншими словами, цей підхід може також спростити і відновити доступ до інформації про самого студента, навіть у випадку втрати носія гаманця, якщо у студента є кодова фраза.

Розробка концепції системи

Один з ключових принципів пропонованої системи полягає у тому, що власником академічних даних здобувача буде сам здобувач, а не надавач освітніх послуг, як у класичних системах, але створення й обробка таких даних буде лягати на інших учасників мережі — себто викладачів, заклади освіти, тощо.

Зважаючи на те, що такі дані можна класифікувати як персональні, оскільки вони будуть містити ідентифікатори здобувача, зокрема такі як прізвище, ім'я, дату народження, тощо такі дані повинні будуть бути захищені від несанкціонованого доступу, що означає неможливість використання блокчейн мережі відкритого типу. Одночасно, одним із завдань даної мережі є забезпечення доступу до інформації про академічні здобутки чи кваліфікацію для третьої сторони, яка зацікавлена в перевірці достовірності даних, відповідно у цьому випадку використання блокчейн мережі закритого типу також є недоцільним. Тому для створення такої системи буде доцільним обрати блокчейн мережу гібридного типу [18], яка поєднує в собі переваги обох типів, тобто така мережа дає змогу одночасно змогу отримати доступ до інформації всім бажаючим, одночасно контролюючи інформацію, яка буде доступною для відкритого доступу. Також, властивість незмінності даних збережених у блокчейн дозволить впевнитися в тому, що у них не вносилися будь-які несанкціоновані зміни, оскільки в мережі не існує користувачів із особливими правами, які могли б це зробити.

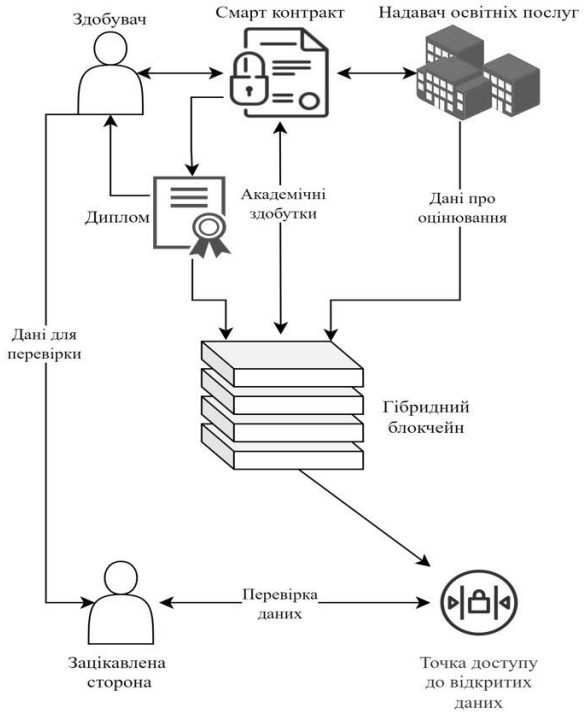

Рис. 2. Концептуальна схема системи

Наступним принципом буде використання технології смарт контрактів для створення даних про академічні здобутки. Тобто саме смарт контракт буде приймати рішення про видачу сертифікату чи диплому, успішне вивчення дисципліни тощо. Тож для забезпечення виконання даного принципу буде використовуватися токенізація навчального процесу, тобто випуск в середині мережі утилітарних токенів [19],

які будуть відігравати роль оцінок, отриманих заліків, тощо. Наприклад, здобувач отримує на власний гаманець токени балів дисципліни за виконані практичні завдання, зданий екзамен тощо і в кінці циклу смарт контракт на основі накопичених токенів буде обмінювати їх на токен дисципліни, який буде містити інформацію про кількість набраних токенів оцінювання (балів) та результат вивчення дисципліни. Також такий підхід можна застосувати і до видачі сертифікату чи диплому, де критерієм буде наявність всіх необхідних токенів дисципліни із статусом, який свідчить про успішне вивчення кожної дисципліни. Маємо схему роботи такої системи (рис. 2).

Алгоритм роботи системи матиме такі кроки:

1. Здобувач отримує крипто гаманець;
2. Надавач освітніх послуг знайомить здобувача із умовами;
3. Між здобувачем та надавачем укладається смарт контракт;
4. Дані про успішність вносяться в блокчейн;
5. Смарт контракт обробляє дані в блокчейн та на основі обробки приймає рішення про успішне вивчення дисципліни чи видачу диплому;
6. Диплом додається у блокчейн, а власником диплому встановлюється здобувач;
7. За необхідності здобувач надає дані диплому зацікавленій стороні для перевірки;
8. Зацікавлена сторона через точку доступу до блокчейн перевіряє надану інформацію.

Отже, даний підхід пропонує використання мережі блокчейн як вмістилища інформації про успішність здобувача, його академічні досягнення тощо. Також відбувається забезпечення доступу до відкритої інформації через точку доступу для будь-кого зацікавленого в отриманні такої інформації чи перевірці достовірності наданої їм інформації, наприклад підтвердження права власності наданого диплому.

Природньо, що незважаючи на переваги системи, така система також буде мати недоліки. Найбільш очевидними недоліками системи будуть ті, які пов'язані із самою технологією блокчейн та смарт контрактами.

Наприклад, суттєвим недоліком для розробки і підтримки даної системи може стати висока вартість смарт контрактів, оскільки ціна завантаження контракту в мережу залежить від його розміру, тобто від кількості програмного коду, який буде завантажено в мережу [20]. Тож, використання смарт контрактів в мережі має певну дуальність в контексті переваги-недоліки, оскільки дана технологія дозволяє виключити людський фактор із процесу видачі сертифікатів, дипломів чи обробки результатів контролю успішності, що дозволяє знизити ризики несанкціонованого втручання та адміністративного навантаження, одночасно збільшуючи ціну розробки та підтримки мережі, через залежність ціни впровадження такого контракту в мережу, затрат на розробку та тестування. Також зважаючи на відносну молодість самої технології, проблемою може стати пошук спеціалістів відповідного рівня. Проблему із ціною та складність коду смарт контрактів можна вирішити шляхом спрощення критеріїв успішності, зменшенням кількості смарт контрактів тощо. Одним із можливих шляхів реалізації цього шляху є відмова від створення смарт контрактів для кожної дисципліни окремо та реалізація лише смарт контрактів, які будуть контролювати лише видачу сертифікатів. Варто зазначити, що збереження даних про успішність однаково має відбуватися в блокчейн, для забезпечення цілісності та незмінності даних. Очевидно, що такий підхід є компромісом, оскільки він вводить додатковий вплив на мережу з боку людини, оскільки рішення про успішне вивчення дисципліни буде прийматися саме зі сторони надавача освітніх послуг (табл. 1).

Таблиця 1

Переваги та недоліки запропонованого методу

Процес аналізу	Система на основі гібридної мережі
Переваги	- здобувач є власником власних даних; - можливість доступу до відкритих даних мережі; - захищеність персональних даних через розмежування доступу; - збереження інформації впродовж всього часу існування системи; - автоматизація видачі дипломів та підтвердження успішного вивчення дисциплін.
Недоліки	- зниження рівня прозорості через гібридну мережу; - зниження рівня децентралізації; - ризик високої вартості смарт контрактів через високу складність контрактів; - необхідність переходу на нову систему, що потребуватиме навчання персоналу; - можливі складнощі міграції даних між різними постачальниками; - постійний ріст розміру блокчейн через ріст кількості користувачів, які пройшли крізь систему; - розробка механізму безпечного зберігання чутливих даних.

Ще одним недоліком даної системи є ріст розміру блокчейн, оскільки природа технології вимагає збереження абсолютно всіх даних, які коли-небуть в неї вносилися. Тут теж можна помітити, що така особливість теж має дуальність у раніше згаданому контексті, оскільки з одного боку розмір мережі буде впливати на швидкодію мережі, а з іншого боку дана властивість дозволить перевірити автентичність даних збережених у будь-який момент існування мережі, навіть якщо вони зберігалися 10, 20 чи 50 років тому, основним критерієм можливості перевірки буде лише сам факт існування мережі [21].

Також складнощі можуть виникнути при потребі міграції даних між надавачами освітніх послуг, наприклад при переході здобувача з одного закладу в

інший. Очевидно, що дана проблема може бути не актуальною для надавачів освітніх послуг, які проводять різні курси, наприклад курси програмування чи кулінарії. Однак, в разі використання такої системи у ЗВО, необхідність подолання даної проблеми одразу стає необхідністю, оскільки повинна бути забезпечена можливість академічної мобільності для всіх учасників освітнього процесу. Відповідно шляхом подолання може стати розробка механізму передачі даних з мережі та внесення даних в мережу, іншими словами — розробка механізму інтеграції системи із системою освіти.

Разом з цим недоліком слід розглядати й можливості складнощів у впровадження даної системи замість наявної [22]. Оскільки при переході на систему, концепція якої тут запропонована, потрібно буде розгорнути не просто сервер для опрацювання даних, а цілу децентралізовану мережу, яка буде забезпечувати функціонування системи, а також провести навчання з роботи із новою системою для всіх, хто задіяний у процесі надання освітніх послуг [23].

Окрім згаданих недоліків, слід зазначити що ще одним викликом буде реалізація механізму безпечного поширення даних для підтвердження дипломів і, взагалі, реалізація відкритої частини гібридного блокчейн, оскільки необхідно чітко визначити не лише необхідний мінімум інформації для підтвердження даних, але й безпечний шлях передачі даних для запобігання розкриттю персональної інформації. Подоланням цього виклику може стати гешування [24] даних та розміщення у відкритому вигляді ідентифікаторів уже у вигляді гешу, що з одного боку дозволить однозначно ідентифікувати власника, а з іншого — не розкрити ідентифікатори особи для широкого загалу. Також перевагою такого підходу буде те, що зацікавлена сторона зможе переконатися не лише в наявності наданої їй інформації в мережі надавача освітніх послуг, але й впевнитися в тому, шо наданий їй геш-ідентифікатор відповідаю саме тій особі, яка його надавала, оскільки результат гешування статичних даних буде завжди однаковим.

Висновки. Аналізуючи проблему застосування технології блокчейн в освіті, було виявлено переваги та недоліки використання цієї технології. По-перше, використання цієї технології може підвищити рівень довіри між учасниками освітнього процесу за рахунок запобігання несанкціонованим змінам даних, а також за рахунок надання студентам можливості керувати інформацією про себе та бачити будь-які зміни, внесені до їхніх профілів. Ще одним важливим аспектом використання цієї технології є те, що наявність цих даних у мережі блокчейн дозволяє зацікавленим сторонам перевіряти такі дані, як надані дипломи та сертифікати.

Використання смарт-контрактів зменшує вплив людського фактору, тим самим знижуючи навантаження на адміністративні відділи ВНЗ та зменшуючи кількість помилок. Однак використання технології має і слабкі сторони, які впливають на її потенціал для використання в освітньому секторі на даному етапі. Зокрема, найбільшою перешкодою може стати зберігання інформації про учасників освітнього процесу в мережі блокчейн. Оскільки така інформація зберігається відкрито в самій мережі, потрібні методи її захисту.

Смарт-контракти коштують недешево, але їх використання необхідне для гарантування роботи системи та мінімізації людського втручання, ціна якого залежить від складності та розміру коду. Оновлення самого коду смарт-контракту також потребує фінансових витрат, оскільки будь-які зміни в навчальній програмі мають бути відображені в Інтернеті, а сам код смарт-контракту - відповідно змінений.

Крім того, з часом зростання самої мережі призведе або до збільшення обчислювальних потужностей, або до зменшення швидкості транзакцій всередині мережі через розмір самого блокчейну.

Однак використання цієї технології в освітній сфері забезпечить автентичність даних, що надаються зацікавленим сторонам, таких як дипломи, сертифікати та ступені, що підтверджують володіння кваліфікацією та необхідними навичками. Таким чином, впровадження технології блокчейн в освітній сфері забезпечить прозорість освітнього процесу, що створить основу для забезпечення довіри між роботодавцями, випускниками та навчальними закладами, що, в свою чергу, сприятиме підвищенню репутації українських вищих навчальних закладів.

Список літератури

[1]. Gilder, G.F. (2018) Life after Google: The fall of big data and the rise of the blockchain economy. Washington, D.C., Regnery Gateway, pp. 6-12.

[2]. Park, J. (2021) Promises and challenges of Blockchain in education. In: Smart Learn Environ, 8(1), p. 33.

[3]. Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. Inamorato dos Santos, A. (ed.). URL: http: // publications.jrc.ec.europa.eu / repository /bitstream/ JRC108255/jrc108255_blockchain_in_education (1).pdf.

[4]. Sharples, M., & Domingue, J. (2016). A Distributed System for Educational Record, Reputation and Reward. Adaptive and Adaptable Learning., pp. 490-496. Cham: Springer. URL: https://link.springer.com/chapter/10.1007% 2F978-3-319-45153-4_48.

[5]. Skiba, D. J. (2017). The potential of Blockchain in education and health care. Nursing education perspectives, Vol. 38, No 4, pp. 220–221.

[6]. Clark, D. (2016). 10 ways blockchain could be used in education. OEB Insights. URL: https://oeb-insights. com / 10-ways-blockchain-could-be-used-in-education/.

[7]. Russell, J. (2017). Sony wants to digitize education records using the blockchain. URL: https:// techcrunch. com/ 2017 / 08 / 09/ sony-education-blockchain.

[8]. Shu, Y. L., Pascal, T. F., Abdullah, A., Omar, M, Laiha, M. K., Tan, F. A., & Reza, I. (2018). Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey. International Journal on Advanced Science, Engineering and Information Technology, Vol. 4-2, pp. 1735-1745. URL: http://ijaseit.insightsociety. org / index. php ? option = com_content & view=article&id=9&Itemid=1&article_id=6838.

[9]. Lewis, A. (2017). A Gentle introduction to self-sovereign identity. URL: https://bitsonblocks.net/2017/05/17/agentle-introduction-to-self-sovereign-identity.

[10]. Universal. Medium. Blockchain in Education. (2018) [Електронний ресурс]. Режим доступу до ресурсу: https: // medium.com / universablockchain / blockchain-in-education-49ad413b9e12.

[11]. Febin John James. Hackernoon. What happens when you combine blockchain and education? (2018) [Електронний ресурс]. Режим доступу до ресурсу: https: // hackernoon.com / what - happens - when-you-combine-blockchain-and-education-d533ef6d4862 12.

[12]. Revolutionizing Education with Smart Contracts (2023) [Електронний ресурс]. Режим доступу до ресурсу: https://medium.com/@solidity101/revolutionizing-education-with-smart-contracts-742e570a414f.

[13]. The Future Of Blockchain Technology In Education (2023) [Електронний ресурс]. Режим доступу до ресурсу: https: // elearningindustry.com/ the-future-of-blockchain-technology-in-education.

[14]. Fekete, D.L.; Kiss, A. (2023) Toward Building Smart Contract-Based Higher Education Systems Using Zero-Knowledge Ethereum Virtual Machine. Electronics 2023, 664 p.

[15]. A Survey on Blockchain for Information Systems Management and Security / D. Berdik та ін. Information Processing & Management. 2021. Т. 58, № 1. с. 102397. URL: https://doi.org/10.1016/j.ipm.2020.102397.

[16]. Khan M., Naz T. Smart Contracts Based on Blockchain for Decentralized Learning Management System. SN Computer Science. 2021. Т. 2, № 4. URL: https://doi.org/10.1007/s42979-021-00661-1 (дата звернення: 28.08.2023).

[17]. Gilbert J. The Seed Phrase Debate: Do Crypto Wallets Actually Need Them? Blockworks. [Електронний ресурс]. Режим доступу до ресурсу: https:// blockworks.co/news/what-are-seed-phrases.

[18]. What we learned from designing an academic certificates system on the Blockchain. (2020) [Електронний ресурс]. Режим доступу до ресурсу: https:// medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-Blockchain 34ba5874f196.

[19]. Security Tokens Vs. Utility Tokens : A Concise Guide [UPDATED] (2023) [Електронний ресурс]. Режим доступу до ресурсу: https: // www.blockchain-council. org / blockchain / security-tokens-vs-utility-tokens-a-concise-guide/.

[20]. Blockchain in Education – Top use cases and potential pitfalls that businesses must know (2023) [Електронний ресурс]. Режим доступу до ресурсу: https: // appinventiv.com / blog / blockchain-in-education/.

[21]. Poberezhnyk, V., Opirskyy, I. Developing of Blockchain Method in Message Interchange Systems (2023) CEUR Workshop Proceedings, 3421, pp. 148-157.

[22]. S. Vasylyshyn, I. Opirskyy, V. Susukailo, Analysis of the use of software baits as a means of ensuring information security, in: 2020 IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT), IEEE, 2020. doi:10.1109/ csit49958. 2020. 9321925.

[23]. Vasylyshyn, S., Susukailo, V., Opirskyy, I., Kurii, Y., & Tyshyk, I. (2023). A model of decoy system based on dynamic attributes for cybercrime investigation. Eastern-European Journal of Enterprise Technologies, 1(9 (121), pp. 6-20. https: // doi.org / 10.15587 / 1729-4061. 2023. 273363

[24]. Blockchain in Education (2023) [Електронний ресурс]. Режим доступу до ресурсу: https://builtin. com/blockchain/blockchain-education.

УДК 004.065

Opirskyy I., Balatska V., Poberezhnyk V. Modern possibilities of use blockchain technology in the education system

Abstract. *Blockchain technology has traditionally attracted attention due to its potential to revolutionize various industries, primarily finance and supply chain management. Education is rarely talked about in this context, but there is something to transform in it, for example, certification, issuing diplomas, certificates. At the same time, blockchain in certification is not just a confirmation of knowledge and academic purity, but a new approach through the creation of a system for storing and distributing information about learning results. This article explores the potential applications of blockchain technology in the education sector, with a focus on unique use cases related to courses, payments, exams and qualifications. Smart contracts are self-sustaining contracts with predefined terms. These contracts run on the blockchain network, eliminating the need for intermediaries and providing trust, transparency and automation. In the education sector, smart contracts can streamline administrative processes, increase security, and ensure a consistent record of achievement. They empower both learners and educational institutions by providing a decentralized platform for learning, assessment and certification. The purpose of the article is to study the possibilities and prospects of using blockchain technology and smart contracts in science and education.*

Key words: *blockchain, smart contract, education, decentralized system, personal data protection.*

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».
Ivan Opirskyy, Dc.S., Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".

Балацька Валерія Сергіївна, аспірант, спеціальності «Кібербезпека та захист інформації» Національного університету «Львівська політехніка».
Valeriia Balatska, Postgraduate the Department of Information Security, National University "Lviv Polytechnic".

Побережник Василь Олегович, аспірант, спеціальності «Кібербезпека та захист інформації» Національного університету «Львівська політехніка».
Vasyl Poberezhnyk, Postgraduate the Department of Information Security, National University "Lviv Polytechnic".

Отримано *1 жовтня 2023 року,* затверджено редколегією *30 жовтня 2023 року*