КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1202
УДК 004.056.5

Партика Андрій Ігорович
кандидат технічних наук, доцент, доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

Совин Ярослав Романович
кандидат технічних наук, доцент, доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0002-5023-8442
yaroslav.r.sovyn@lpnu.ua

РОЗРОБКА КОНЦЕПЦІЇ ОПТИМІЗОВАНОГО МЕТОДУ ЗАСТОСУВАННЯ БЛОКЧЕЙН ІЗ ЗАБЕПЕЧЕННННЯ АНОНІМНОСТІ ДЛЯ ЗАСТОСУВАННЯ У ЖУРНАЛАХ ОБЛІКУ ВІДВІДУВАНОСТІ

Анотація. Ця стаття присвячена розгляду проблеми забезпечення захисту приватних даних користувачів у системах обліку відвідуваності, які використовують блокчейн та методу оптимізації навантаження на мережу і використання ресурсів. Більшість досліджень, які спрямовані на інтеграцію блокчейн в системи обліку, не досліджують проблеми пов’язані із приватністю користувачів і використанням ресурсів, однак більше сфокусовані на проблемах застосування смарт контрактів для забезпечення роботи цих систем. У цьому дослідженні увагу спрямовано саме на вирішення проблем оптимізації і приватності. Для цього було запропоновано метод створення децентралізованих облікових записів, які дозволяють підтвердити особу, яка ними володіє, а за замовчуванням приховувати особисті дані розпорядника децентралізованого ідентифікатора. Запропоновано метод обліку відвідуваності який орієнтований на оптимізацію використання ресурсів мережі шляхом розмежування методів обробки даних — використання on-chain та off-chain обробки. Суть цього методу полягає у збереженні даних у IPFS, а доказів їхньої достовірності – у блокчейн, що дозволяє одночасно забезпечувати їхню доступність і незмінність через характеристики IPFS та блокчейн. Проведене моделювання оцінки навантаження дозволило підтвердити дієвість запропонованого методу для зниження навантаження на мережу, а використання децентралізованих ідентифікаторів із використанням запропонованого анонімного ідентифікатора, який створюється із набору персональних даних та криптографічної солі, у складі децентралізованого ідентифікатора дозволяє забезпечити збереження приватності користувачів, що дозволяє розглядати запропонований метод як теоретичну основу для подальших досліджень і розробки систем обліку відвідуваності на основі комбінації блокчейн та IPFS.

Ключові слова: блокчейн; приватність; анонімність; IPFS; смарт контракти; відвідуваність; хешування; децентралізований ідентифікатор.

ВСТУП

Стрімка цифровізація освітніх процесів вимагає надійних інструментів для контролю відвідуваності. Ця необхідність зумовлена тим, що відвідуваність має позитивний вплив на академічні здобутки [1], а контроль відвідуваності дає можливість забезпечити раннє виявлення проблем із успішністю і протидіяти їм [2].Традиційні централізовані системи контролю доступу (наприклад, журнали на базі реляційних баз даних або RFID-систем) мають фундаментальні вразливості: вони схильні до несанкціонованих маніпуляцій з даними, мають єдину точку відмови та не забезпечують прозорості для незалежного аудиту. Впровадження технології блокчейн

дозволяє вирішити проблему довіри завдяки створенню незмінного та прозорого реєстру подій.

Постановка проблеми. Застосування блокчейн і автоматизації через застосування смарт контрактів є потужним механізмом, який дозволяє забезпечувати збереження важливих даних надійним способом [3],[4]. Однак, однією з проблем рішень на основі блокчейн є оптимізації процесів. Ця проблема зумовлена тим, що вартість обробки блокчейн і складність лінійно зростає із кількістю учасників мережі: якщо припустити, що середня кількість пар на день дорівнює чотирьом у групі студентів із 30, то за день кількість транзакцій, які будуть додані у блокчейн, буде становити, як мінімум, 124 транзакції: 120 – від студентів, 4 – викладачі, які проводили заняття і також реєстрували свою присутність. Цього достатньо, щоб припустити те, що збереження всіх даних у блокчейн є низькоефективним рішенням у контексті оптимальності, оскільки кількість транзакцій і ціна обробки мережі стрімко зростає із кількістю учасників, які виконують дії, спрямовані на додавання даних у блокчейн.

Інша важлива проблема, яку потрібно вирішити у контексті застосування блокчейн, – це забезпечення приватності користувачів такої системи, що часто конфліктує з відкритістю мережі блокчейн, яка сама конфліктує із різними нормами, наприклад “Право на забуття”, яке регламентується нормами GDPR [5], або п.8 ст.6 Закону України “Про захист персональних даних”, який вимагає те, щоб дані оброблялися не довше, ніж це потрібно [6]. Тобто існує необхідність забезпечення можливості видалення персональних даних із системи, що суперечить природі технології блокчейн, однією з властивостей якої є незмінність даних доданих у мережу, що унеможливлює таке видалення з мережі.

Аналіз останніх досліджень і публікацій. Дослідження [7-9] демонструють способи застосування технології блокчейн і смарт контрактів у сфері освіти, зокрема для підтвердження даних академічної успішності чи отриманих дипломів, кваліфікацій тощо. Однак вони орієнтовані на застосування смарт контрактів чи NFT, що означає використання великої кількості транзакцій, що є проблемою масштабування системи і оптимізації витрати ресурсів [8] при необхідності обробки значних обсягів даних щодня.

Інші дослідження [10], [11] пропонують методи вирішення проблема масштабування систем основаних на засобах блокчейн через розподіл обробки даних на off-chain та on-chain системи, що дозволяє вирішити проблему масштабування зберігаючи дані поза блокчейн, а сам блокчейн використовувати для збереження доказів достовірності даних.

Також інші дослідження [12], [13] пропонують спосіб вирішення проблем приватності персональних даних користувачів шляхом використання децентралізованих ідентифікаторів, що дозволяє забезпечити приватність облікових даних.

Отже, інтеграція цих методів дозволяє розробити метод, який буде вирішувати проблему захисту приватності користувачів і оптимізації використання ресурсів в системах основаних на блокчейн.

Метою статті є розробка оптимізованого методу обробки даних обліку відвідуваності із використанням децентралізованого зберігання даних та підтвердженням достовірності через блокчейн, який забезпечує збереження приватності учасників мережі на основі застосування засобів децентралізованих ідентифікаторів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Суть пропонованої концепції методу полягає у застосуванні блокчейн як провайдера достовірності даних у системі шляхом збереження доказів незмінності даних у off-chain сховищі, роль якого відіграє IPFS. В свою чергу захист приватності користувачів відбувається через застосування приховування їхніх особистостей через криптографічні ідентифікатори на основі децентралізованих ідентифікаторів.

Перевага децентралізованих ідентифікаторів у тому, що вони дозволяють передати керування обліковим записом користувача самому користувачу, а роль установи звести до провайдера облікових даних. Зважаючи на те, що ці облікові записи використовуються для підтвердження присутності, то вони повинні базуватися на парадигмі верифікованих облікових записів (verifiable credentials), які є частиною множини децентралізованих ідентифікаторів. Такі ідентифікатори дозволяють пересвідчитися в тому, що йому можна довіряти, що дозволяє застосовувати його в системах, які потребують керування правами доступу [14].

Досягти того, щоб децентралізований ідентифікатор вважався довіреним можна кількома способами: збереженням відбитку ідентифікатора у блокчейн або використанням цифрових підписів, які дозволяють пересвідчитись у тому, що дані були створені сутністю, яка володіє необхідними правами. У контексті реєстрації відвідуваності занять, такою сутністю може бути сам заклад освіти або його структурна одиниця, наприклад катедра чи інститут.

Іншим аспектом використання децентралізованих ідентифікаторів є те, що їх можна використовувати не лише для ідентифікації користувачів системи, а для будь-якої сутності у системі [15], [16], що дозволяє їх застосовувати для створення децентралізованих ідентифікаторів для структурних одиниць закладу освіти. Такий підхід дозволяє створити ієрархічну структуру, де центральний орган управління закладу освіті відіграє роль провайдера ідентифікаторів для структурних одиниць, а структурні одиниці – для користувачів мережі, що зображено на рисунку 1.

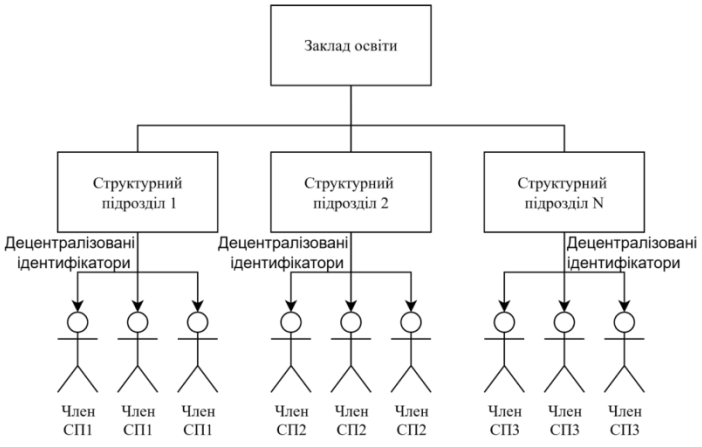

Рис. 1. Ієрархічна структура

Це дозволяє масштабування для зручності застосування такого методу до установ різного розміру, що обумовлено тим, що створення таких користувачів однією установою може викликати як перевантаження адміністративного персоналу, оскільки потребує обробки багатьох користувачів, а також тим, що розподіл користувачів на

своєрідні кластери, дозволяє краще керувати ідентифікаторами зберігаючи ланцюг підтвердження довіри.

При такому підході важливим є створення ідентифікатора користувача, який дозволяє чітко ідентифікувати користувача при потребі і одночасно забезпечувати його анонімність при користуванні системою. Для вирішення цієї проблеми можна скористатися засобами криптографічних перетворень – хешуванням.

Перевага застосування хешування полягає в тому, що функції хешування є односторонніми і не дозволяють відновити із них початкові дані, а також дозволяють завжди отримувати один і той самий результат, при використанні хешування на різних системах. Однак застосування лише такого методу не гарантує захист персональних даних, оскільки хеш-суми і можливий набір вхідних даних, у цьому випадку членів структурних підрозділів (студенти і викладачі), може дозволити отримати ідентифікатор для конкретної особи використанням звичайного перебору. Для протидії цьому можна застосувати засоби, які використовуються при збереженні хешів паролів користувачів у класичних системах керування доступом, – використання криптографічної солі:

$$IDA = H(PII, S) \quad (1)$$

де ID_A – анонімізований ідентифікатор, H – функція хешування, PII – персональні дані, наприклад ім'я, прізвище, група тощо, S – криптографічна сіль.

Це дозволить захистити особистість власника від атак перебору, а збереження солі – підтвердити власника ідентифікатора при необхідності, що досягається через обчислення хеш-суми з переданих PII та збереженої криптографічної солі. Це дає можливість створити децентралізований ідентифікатора, який буде застосовувати в системі обліку відвідуваності.

Сутність такого ідентифікатора можна представити наступним виразом:

$$DID = \{ID_A,\ K_{pub},\ K_{priv},\ \sigma_U\} \quad (2)$$

де DID – децентралізований ідентифікатор, K_{pub} – публійний ключ, K_{priv} – приватний ключ, σ_U – підпис того, хто видав ідентифікатор. Такий набір параметрів дозволить забезпечувати можливість подавати звітність про власне відвідування шляхом використання інфраструктури публічних ключів.

Фактом того, що особа була присутня є розв'язане завдання від системи контролю присутності, наприклад цифровий підпис згенерований на основі випадкового числа, яке генерується при перевірці присутності. Для оптимізації цього процесу, запропоновано підхід пакетної обробки, замість реєстрації кожного підпису окремо.

Застосування IPFS дозволяє вирішити одночасно два завдання: перенести збереження даних за межі блокчейн і створити докази незмінності збережених даних. Оскільки IPFS використовує адресацію на основі контенту, яка ґрунтується на засобах хешування, то будь-яка зміна у даних призводить до лавинних змін у ідентифікаторі IPFS – CID [17]. Цей аспект дозволяє використовувати CID не лише для отримання даних із мережі IPFS, але й як доказ незмінності, оскільки змінені дані призводять до генерації нового ідентифікатора, а не зміни даних, які знаходяться за оригінальним CID. Також застосування IPFS гарантує безпечне збереження даних, яке гарантує доступність даних [18].

Поєднання збереження даних в IPFS і зберігання відбитків даних у блокчейн, дозволяє отримати стійкі докази цілісності та достовірності даних, оскільки дані збережені у блокчейн не можуть бути зміненими несанкціоновано, що дозволяє отримати гарантію достовірності даних. Запис у блокчейн можна охарактеризувати таки виразом:

$$T = \{CID_L, \sigma_U\} \tag{3}$$

де T – транзакція, яка додається в блокчейн, CID_L – ідентифікатор переліку присутність в IPFS, σ_U – підпис того, хто додає транзакцію (кафедра, інститут тощо). У свою чергу CID_L формується так:

$$CID_L = IPFS_{add}(P_{register}(a_1, a_2, \dots a_n)) \tag{4}$$

де $IPFS_{add}$ – функція додавання в IPFS, $P_{register}$ – функція реєстрації присутніх, $a_1 \dots a_n$ – присутні. Для реєстрації присутності функція використовує цифрові підписи, тобто для реєстрації присутності, необхідно згенерувати цифровий підпис із застосування приватного ключа, який є частиною децентралізованого ідентифікатора описаного у виразі 1. Відповідно для кожного пристунього генерується окремий nonce, який потім зберігається разом із підписом у єдиному файлі, який містить перелік усіх присутніх, що схематично зображено на рисунку 2.

Перелік пристуніх
ID_{A1}:$nonce_1$:σ_1
ID_{A2}:$nonce_2$:σ_2
...
ID_{A3}:$nonce_3$:σ_3

Рис. 2. Схематичне зображення переліку присутніх

Структура зображена на рисунку 2 дозволить не лише зберегти дані, але й при потребі перевірити справжність підписів, оскільки дозволяє встановити відповідність між підписом і його власником, не розкриваючи при цьому жодних персональних даних.

Користуючись принципами описаними у виразах можна розробити математичну модель перевірки присутності:

$$Verify = \begin{cases} 1, & ID_{AN} \in IPFS_{get}(CID_{LN}) \wedge S(nonce_{AN}, K_{priv}^{AN}) = \sigma_{IPFS_{get}(CID_{LN})}^{AN} \\ 0 \end{cases} \tag{5}$$

де $Verify$ – результат перевірки, ID_{AN} – анонімний ідентифікатор користувача, якого перевіряють, $IPFS_{get}$ – функція отримання даних з IFPS, CID_{LN} – ідентифікатор даних відвідуваності, які перевіряють, S – функція генерування підпису, $nonce_{AN}$ – nonce використаний для генерації підпису, $\sigma_{IPFS_{get}(CID_{LN})}^{AN}$ – збережений підпис користувача, якого перевіряють. Описані методи дозволяють створити мінімальний набір засобів для функціонування системи.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Для оцінки навантаження на систему було порівняно підходи, які пропонуються іншими рішенням для обліку, наприклад, коли за допомогою смарт контрактів фіксують присутність. При такому підході кожен учасник мережі для підтвердження виконує транзакцію, яка зберігається у блокчейн. При такому підході використання ресурсів можна охарактеризувати наступним виразом:

$$R_c = \sum_{i=1}^{D} \sum_{j=1}^{N_D} (U_j \times T_j \times P) \tag{6}$$

де R_c– загальні використані ресурси, U_j – і-користувач системи, T_j – кількість транзакцій, які згенеровані і-користувачем, P – використання ресурсів на транзакцію, N – кількість активних користувачів, D – кількість днів, коли робили записи.

При використанні запропонованого методу використання ресурсів оцінюється наступним виразом:

$$R_o = \sum_{i=1}^{D} \sum_{j=1}^{S} (U_S \times P) \tag{7}$$

де R_O – кількість ресурсів при оптимізованому підході, S – кількість структурних підрозділів. Також тут P – це значення із умовними одиницями вимірювання, оскільки залежно від типу блокчейн, воно може змінюватися, тому у цих розрахунках воно представляє умовні одиниці навантаження.

Для моделювання використання ресурсів обрано такі параметри: кількість днів, коли відбувалася реєстрація 175, кількість студентів – 30, середня кількість пар на день – 4, кількість інститутів, які подають звітність – 5. Результати моделювання використання ресурсів наведено на рисунку 3.

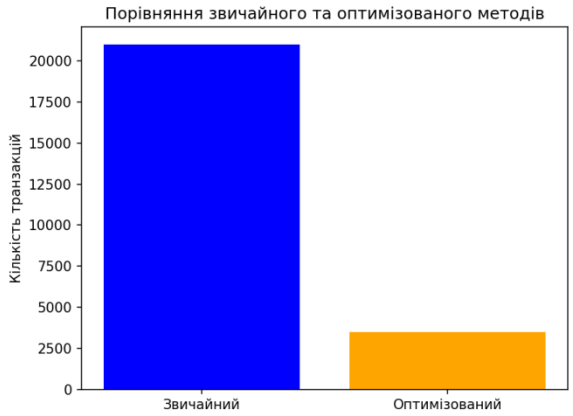

Рис. 3. Порівняння навантаження при оптимізованому і звичайному підходах

Це порівняння демонструє суттєве зниження навантаження на блокчейн, оскільки при оптимізованому підході транзакції в мережу додає не кожен відвідувач окремо, а структурний підрозділ збирає пакет і записує одну транзакцію в блокчейн, яка дозволяє підтвердити достовірність даних про відвідуваність, зберігаючи самі дані у IPFS.

Опісля було проведено моделювання навантаження для сценаріїв, коли кількість студентів, які звітують про присутність була: 100, 1000, 5000, 10000, 20000, 50000. Для кількості інститутів значення були такими: 1, 5, 10, 20, 50, 100. Решту параметрів, залишилися незмінними: середня кількість пар – 4, кількість днів, коли було звітування – 175. Результати моделювання наведено на рисунку 4.

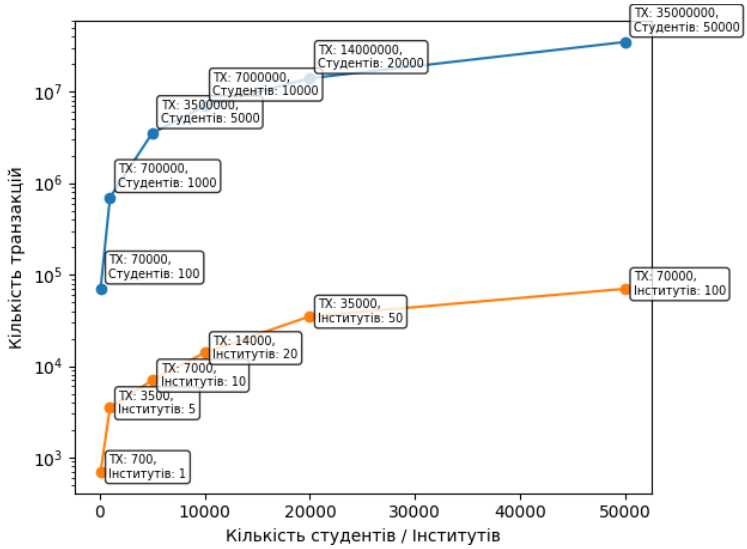

Рис. 4. Результати моделювання росту навантаження

Це моделювання дозволяє підтвердити ефективність запропонованого методу оптимізації на основі пакетної обробки, оскільки при такому методі навантаження залежить не від кількості осіб, які реєструють свою присутність, а від кількості структурних підрозділів, які подають цю звітність у вигляді пакетів даних.

На додачу, запропонована організаційна структура, яка використовує ієрархічність структури закладу освіти, де найвищим є центральний орган управління, а найнижчим особа, яка звітує про присутність, дозволяє масштабувати пропонований метод для організацій різного розміру, наприклад використовувати кафедри як провайдерів звітності або навпаки укрупнити до рівня інституту, факультету тощо. Однак тут слід наголосити на тому, шо збільшення кількість провайдерів звітності збільшує навантаження на мережу, тому потрібно підтримувати баланс між кількістю таких провайдерів і навантаженням на мережу.

Окрім цього використання запропонованих методів анонімізації, дозволяють узгодити використання блокчейн і вимоги законодавства щодо захисту персональних даних. Застосування децентралізованих ідентифікаторів дозволяє перенести керування ними на сторону користувача і одночасно використовувати безпечний ідентифікатор, який не пов’язаний із особистістю напряму, а застосування запропонованого ідентифікатора ID_A дозволяє відновити при необхідності дані про особистість.

Запропонований метод дозволяє оптимізувати використання ресурсів мережі через розподіл обробки даних на on-chain та off-chain частини, що дозволяє суттєво знизити навантаження на мережу блокчейн і можливі фінансові витрати, оскільки кількість транзакцій зменшується до мінімально необхідної кількості шляхом застосування підходу пакетної обробки даних відвідуваності. Окрім цього, запропоновано метод вирішення проблеми приватності користувачів шляхом застосування децентралізованих ідентифікаторів, які дозволяють забезпечувати точне відслідковування даних відвідуваності кожною конкретною особою одночасно

забезпечуючи збереження приватності користувача, що дозволяє забезпечити виконання вимог GDPR та Закону України “Про захист персональних даних”, оскільки сам децентралізований ідентифікатор є не пов’язаний із жодними персональними даними користувача на пряму.

Результати цього дослідження дозволять покласти теоретичну основу для розробки оптимізованих для роботою із блокчейн систем обліку відвідуваності, які дозволяють забезпечувати виконання вимог законодавства в області захисту персональних даних.

Запропоновані методи і засоби у цій статті також відкривають низку перспектив для подальших досліджень. Одним з таких можливих напрямків досліджень є дослідження методів захисту від атака на основі MITM та спуфінгу на рівні мережі для забезпечення достовірності інформації. Тут проблема полягає в тому, що запропонований метод покладається на те, що учасники самі повинні надавати інформацію про свою присутність, а це відкриває можливість для недоброчесного заповнення таких даних, наприклад через створення підписів поза межами навчальної аудиторії.

Іншим напрямком є дослідження ефективних механізмів управління і аналізу присутності, оскільки анонімізовані ідентифікатори дозволяють відслідковувати присутність конкретного учасника, однак вони не дозволяють визначити особу, якій вони належать, що є важливим аспектом для відслідковування академічної успішності і прогнозування можливих ризиків пов’язаних із низьким рівнем відвідування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kim, A. S. N., Shakory, S., Azad, A., Popovic, C., & Park, L. (2019). Understanding the impact of attendance and participation on academic achievement. *Scholarship of Teaching and Learning in Psychology*. https://doi.org/10.1037/stl0000151
2. Sälzer, C., Ricking, H., & Feldhaus, M. (2024). Addressing school absenteeism through monitoring: A review of evidence-based educational policies and practices. *Education Sciences, 14*(12), 1365. https://doi.org/10.3390/educsci14121365
3. Chikov, I. A., Koliadenko, S. V., Supryhan, V. A., Tabenska, O. I., Nitsenko, V. S., & Holinko, O. V. (2023). Smart contracts and business process automation: The technical aspect. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 5*, 186–192. https://doi.org/10.33271/nvngu/2023-5/186
4. Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University – Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2021.08.005
5. GDPR.eu. (n.d.). *Everything you need to know about the “right to be forgotten”*. https://gdpr.eu/right-to-be-forgotten/
6. Verkhovna Rada of Ukraine. (2025). *Law of Ukraine “On personal data protection” (No. 2297-VI)*. https://zakon.rada.gov.ua/laws/show/2297-17#Text
7. Opirskyi, I., Balatska, V., & Poberezhnyk, V. (2023). Modern possibilities of using blockchain technology in the education system. *Information Security*, *29*(3), 138–146. https://doi.org/10.18372/2225-5036.29.18073
8. El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., & Shams, M. Y. (2023). Unlocking the power of blockchain in education: An overview of innovations and outcomes. *Blockchain: Research and Applications*, 100165. https://doi.org/10.1016/j.bcra.2023.100165
9. Bhawna, Gupta, P., & Rai, P. (2025). Can blockchain revolutionize educational practices? An in-depth analysis of applications and challenges. *Sustainable Futures, 10*, 101171. https://doi.org/10.1016/j.sftr.2025.101171
10. Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Applied Sciences, 15*(6), 3225. https://doi.org/10.3390/app15063225

11. Fernández-Iglesias, M. J., Delgado von Eitzen, C., & Anido-Rifón, L. (2024). Efficient traceability systems with smart contracts: Balancing on-chain and off-chain data storage for enhanced scalability and privacy. *Applied Sciences, 14*(23), 11078. https://doi.org/10.3390/app142311078
12. Kyriakidou, C. D. N., Papathanasiou, A. M., & Polyzos, G. C. (2023). Decentralized identity with applications to security and privacy for the Internet of Things. *Computer Networks and Communications*. https://doi.org/10.37256/cnc.1220233048
13. Saravanan, V., A, S., Reddy, D. N., Ahamed, B. S., K, U., & M, A. P. (2024). Exploring decentralized identity verification systems using blockchain technology: Opportunities and challenges. In *2024 IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1–6). https://doi.org/10.1109/GCAT62922.2024.10923936
14. Pandiyarajan, A., Jagatheesaperumal, S. K., Rahouti, M., Chehri, A., & Hafid, A. (2025). Decentralized and dynamic self-sovereign identity and attribute-based access control system for privacy management. *IEEE Internet of Things Magazine, 8*(4), 132–139. https://doi.org/10.1109/iotm.001.2400161
15. Dinh-Tuan, H., Garzon, S. R., & Fu, J. (2024). Secure and trustful cross-domain communication with decentralized identifiers in 5G and beyond. In *2024 International Conference on Innovation in Clouds, Internet and Networks (ICIN)*. https://doi.org/10.1109/icin60470.2024.10494437
16. Pino, A., Margaria, D., & Vesco, A. (2023). Combining decentralized identifiers with proof of membership to enable trust in IoT networks. In *2023 International Telecommunication Networks and Applications Conference (ITNAC)*. https://doi.org/10.1109/itnac59571.2023.10368540
17. IPFS Documentation. (n.d.). *Content identifiers (CIDs).* https://docs.ipfs.tech/concepts/content-addressing/
18. Jain, S., Agarwal, A., Pathak, M., & Doriya, R. (2025). Enhanced blockchain and IPFS-based secure storage and sharing of electronic healthcare records. *Cluster Computing, 28*(14). https://doi.org/10.1007/s10586-025-05564-x

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Andrii Partyka
Ct.S., Docent, Docent of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

Yaroslav Sovyn
Ct.S., Docent, Docent of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-5023-8442
yaroslav.r.sovyn@lpnu.ua

DEVELOPMENT OF A CONCEPT OF AN OPTIMIZED METHOD OF USING BLOCKCHAIN WITH ANONYMITY PRESERVATION FOR USE IN THE ATTENDANCE REGISTER

Abstract. This article considers the problem of ensuring the protection of users' private data in attendance accounting systems that use blockchain and a method for optimizing network load and resources usage. Most studies aimed at integrating blockchain into accounting systems do not investigate problems related to user privacy and resource use but are more focused on the problems of using smart contracts to ensure the operation of these systems. In this study, attention is paid specifically to solving optimization and privacy problems. For this purpose, a method for creating decentralized accounts was proposed that allows confirming the person who owns them and hiding the personal data of the decentralized identifier administrator by default. A method for attendance accounting is proposed that is focused on optimizing the use of network resources by distinguishing data processing methods - the use of on-chain and off-chain processing. The essence of this method is to store data in IPFS, and evidence of their authenticity in the blockchain, which allows to ensure simultaneously availability and immutability of the data due by the characteristics of IPFS and blockchain.
The load assessment modeling conducted confirmed the effectiveness of the proposed method for reducing the load on the network. Also, the use of decentralized identifiers using the proposed anonymous identifier, which is created from a set of personal data and a cryptographic salt, as part of the decentralized identifier allows the preservation of user privacy, which allows us to consider the proposed method as a theoretical basis for further research and development of attendance accounting systems based on the combining the blockchain and IPFS.

Keywords: blockchain; privacy; anonymity; IPFS; smart contracts; attendance; hashing; decentralized identifier.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Kim, A. S. N., Shakory, S., Azad, A., Popovic, C., & Park, L. (2019). Understanding the impact of attendance and participation on academic achievement. *Scholarship of Teaching and Learning in Psychology*. https://doi.org/10.1037/stl0000151
2. Sälzer, C., Ricking, H., & Feldhaus, M. (2024). Addressing school absenteeism through monitoring: A review of evidence-based educational policies and practices. *Education Sciences*, *14*(12), 1365. https://doi.org/10.3390/educsci14121365
3. Chikov, I. A., Koliadenko, S. V., Supryhan, V. A., Tabenska, O. I., Nitsenko, V. S., & Holinko, O. V. (2023). Smart contracts and business process automation: The technical aspect. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, *5*, 186–192. https://doi.org/10.33271/nvngu/2023-5/186
4. Shrimali, B., & Patel, H. B. (2021). Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University – Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2021.08.005
5. GDPR.eu. (n.d.). *Everything you need to know about the "right to be forgotten"*. https://gdpr.eu/right-to-be-forgotten/

6. Verkhovna Rada of Ukraine. (2025). *Law of Ukraine "On personal data protection" (No. 2297-VI)*. https://zakon.rada.gov.ua/laws/show/2297-17#Text
7. Opirskyi, I., Balatska, V., & Poberezhnyk, V. (2023). Modern possibilities of using blockchain technology in the education system. *Information Security*, *29*(3), 138–146. https://doi.org/10.18372/2225-5036.29.18073
8. El Koshiry, A., Eliwa, E., Abd El-Hafeez, T., & Shams, M. Y. (2023). Unlocking the power of blockchain in education: An overview of innovations and outcomes. *Blockchain: Research and Applications*, 100165. https://doi.org/10.1016/j.bcra.2023.100165
9. Bhawna, Gupta, P., & Rai, P. (2025). Can blockchain revolutionize educational practices? An in-depth analysis of applications and challenges. *Sustainable Futures*, *10*, 101171. https://doi.org/10.1016/j.sftr.2025.101171
10. Eren, H., Karaduman, Ö., & Gençoğlu, M. T. (2025). Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review. *Applied Sciences*, *15*(6), 3225. https://doi.org/10.3390/app15063225
11. Fernández-Iglesias, M. J., Delgado von Eitzen, C., & Anido-Rifón, L. (2024). Efficient traceability systems with smart contracts: Balancing on-chain and off-chain data storage for enhanced scalability and privacy. *Applied Sciences*, *14*(23), 11078. https://doi.org/10.3390/app142311078
12. Kyriakidou, C. D. N., Papathanasiou, A. M., & Polyzos, G. C. (2023). Decentralized identity with applications to security and privacy for the Internet of Things. *Computer Networks and Communications*. https://doi.org/10.37256/cnc.1220233048
13. Saravanan, V., A, S., Reddy, D. N., Ahamed, B. S., K, U., & M, A. P. (2024). Exploring decentralized identity verification systems using blockchain technology: Opportunities and challenges. In *2024 IEEE Global Conference for Advancement in Technology (GCAT)* (pp. 1–6). https://doi.org/10.1109/GCAT62922.2024.10923936
14. Pandiyarajan, A., Jagatheesaperumal, S. K., Rahouti, M., Chehri, A., & Hafid, A. (2025). Decentralized and dynamic self-sovereign identity and attribute-based access control system for privacy management. *IEEE Internet of Things Magazine*, *8*(4), 132–139. https://doi.org/10.1109/iotm.001.2400161
15. Dinh-Tuan, H., Garzon, S. R., & Fu, J. (2024). Secure and trustful cross-domain communication with decentralized identifiers in 5G and beyond. In *2024 International Conference on Innovation in Clouds, Internet and Networks (ICIN)*. https://doi.org/10.1109/icin60470.2024.10494437
16. Pino, A., Margaria, D., & Vesco, A. (2023). Combining decentralized identifiers with proof of membership to enable trust in IoT networks. In *2023 International Telecommunication Networks and Applications Conference (ITNAC)*. https://doi.org/10.1109/itnac59571.2023.10368540
17. IPFS Documentation. (n.d.). *Content identifiers (CIDs)*. https://docs.ipfs.tech/concepts/content-addressing/
18. Jain, S., Agarwal, A., Pathak, M., & Doriya, R. (2025). Enhanced blockchain and IPFS-based secure storage and sharing of electronic healthcare records. *Cluster Computing*, *28*(14). https://doi.org/10.1007/s10586-025-05564-x

Отримано редакцією журналу / Received: 21.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26