https://doi.org/10.31891/2219-9365-2026-85-28
УДК 004.056.55:004.77:004.91

ГРИЩЕНКО Вадим
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0009-0004-4212-6661
komarda47@fmail.com

МОДЕЛЬ ЗБЕРІГАННЯ ТА ВЕРИФІКАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ НА ОСНОВІ РОЗПОДІЛЕНОГО РЕЄСТРУ ДЛЯ ПІДВИЩЕННЯ ДОВІРИ

У статті запропоновано модель зберігання та верифікації персональних даних на основі технології розподіленого реєстру (блокчейну), орієнтовану на підвищення довіри до цифрових сервісів. Розглянуто архітектуру системи, що включає модулі збору, шифрування, запису метаданих у блокчейн, контроль доступу за допомогою смарт-контрактів і алгоритми перевірки цілісності даних без їх розкриття. Описано формат блоку для запису, модель управління правами доступу на основі мультипідпису та реалізацію політик доступу у вигляді смарт-контрактів. Проведено експериментальне тестування продуктивності моделі в середовищі Hyperledger Fabric із використанням типових сценаріїв, зокрема перевірки освітніх і медичних записів, електронної ідентифікації тощо. Отримані результати свідчать про високу швидкість верифікації, низьке ресурсне навантаження та масштабованість. Запропоноване рішення демонструє наукову новизну завдяки поєднанню механізмів zero-knowledge proof, гнучких політик доступу й інтеграції з зовнішніми цифровими платформами через API. Розроблена модель може бути основою для створення довірених цифрових інфраструктур у сфері електронного врядування, охорони здоров'я та фінансів.

Ключові слова: розподілений реєстр, персональні дані, блокчейн, верифікація, смарт-контракт, криптографічний захист.

HRYSHCHENKO Vadym
Open International University of Human Development Ukraine

A DISTRIBUTED REGISTRY-BASED MODEL OF PERSONAL DATA STORAGE AND VERIFICATION TO INCREASE TRUST

This paper presents a comprehensive model for secure storage and verification of personal data based on distributed ledger technology, specifically blockchain. The proposed architecture addresses the challenges associated with traditional centralized systems, such as data breaches, limited transparency, and lack of user control. The model integrates multiple functional modules: data collection, encryption, block formation, access control via smart contracts, and integrity verification using cryptographic proofs.

The system stores only metadata – such as hashes, timestamps, and identifiers – on the blockchain, while sensitive data remains encrypted and stored separately. Access to data is managed through customizable smart contracts that support dynamic access policies and multisignature authorization schemes. Verification of data integrity can be performed without revealing the content, using methods like hash comparison and zero-knowledge proof.

The model has been tested in a simulated Hyperledger Fabric environment, demonstrating high performance, minimal resource consumption, and scalability. A comparison with centralized and hybrid solutions highlights the advantages of the proposed system in terms of transparency, privacy preservation, and automation of access control.

This research contributes to the development of trusted digital infrastructures by combining decentralization, cryptographic protection, and flexible policy enforcement. The proposed model has strong potential for application in e-governance, healthcare, finance, and education, where trust, security, and privacy are essential.

Keywords: distributed ledger, personal data, blockchain, verification, smart contract, cryptographic protection.

Стаття надійшла до редакції / Received 09.01.2026
Прийнята до друку / Accepted 30.01.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Зростання кількості цифрових сервісів, які оперують персональними даними користувачів, зумовлює підвищення вимог до їх захисту, цілісності та прозорості зберігання [1]. Поширення витоків інформації, зловживання персональними даними та недостатній контроль над їх використанням знижують рівень довіри користувачів до цифрових платформ. У традиційних централізованих системах зберігання даних ключові проблеми пов'язані з уразливістю до зовнішніх атак, внутрішніх зловживань, а також складністю перевірки достовірності інформації без залучення довірених третіх сторін. Це особливо критично в таких сферах, як електронне врядування, фінансові сервіси, охорона здоров'я, де недовіра до систем може призвести до серйозних соціальних, правових і економічних наслідків [2].

Водночас зростає інтерес до технологій розподіленого реєстру, зокрема блокчейну, як до інструменту, що забезпечує незмінність записів, децентралізоване управління та прозорість операцій [3]. Завдяки своїм властивостям, розподілений реєстр може слугувати основою для побудови довірених систем зберігання персональних даних, у яких кожна операція фіксується незмінним чином і може бути верифікована незалежними сторонами без потреби в централізованому контролі. Використання такого підходу дозволяє

зменшити ризики фальсифікації, забезпечити цілісність даних та надати користувачам більший контроль над їх персональною інформацією.

Однак розробка ефективної моделі зберігання та верифікації персональних даних на основі розподіленого реєстру пов'язана з низкою наукових і прикладних завдань. Серед них – визначення структури даних, які підлягають збереженню у реєстрі; забезпечення балансу між прозорістю та конфіденційністю; інтеграція з існуючими цифровими платформами; мінімізація витрат на обчислення та зберігання; а також реалізація механізмів доступу, контролю змін і верифікації достовірності інформації. Такі завдання потребують міждисциплінарного підходу з урахуванням вимог до інформаційної безпеки, криптографічного захисту, архітектури розподілених систем та вимог законодавства щодо обробки персональних даних.

Метою дослідження є розробка моделі зберігання та верифікації персональних даних на основі розподіленого реєстру, орієнтованої на підвищення рівня довіри користувачів до цифрових сервісів.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

У науковій літературі все більше уваги приділяється питанням захисту персональних даних та підвищення довіри до цифрових платформ [4]. Значна кількість досліджень фокусується на вразливостях централізованих систем зберігання, де саме централізація розглядається як головна причина витоків даних, внутрішніх загроз та низької прозорості. Дослідники підкреслюють, що у випадку з персональними даними особливо важливим є не лише захист від зовнішніх атак, а й гарантована можливість користувача контролювати обсяг, спосіб і мету використання власної інформації [5].

З появою технологій розподіленого реєстру, зокрема блокчейну, з'явилася нова парадигма підходів до зберігання й обміну даними. У публікаціях останніх років активно обговорюються переваги таких систем, серед яких: незмінність записів, децентралізація, автоматизована верифікація транзакцій та прозорість історії змін. Роботи [6, 7] описують концепцію використання блокчейн-технологій як основи для децентралізованого зберігання особистих даних, вказуючи на переваги застосування смарт-контрактів для керування доступом до них.

Окрему увагу приділено моделі самоідентифікації (Self-Sovereign Identity, SSI), яка дозволяє користувачам повністю контролювати свої ідентифікаційні дані [8]. У рамках цієї моделі дані можуть зберігатися в розподіленому реєстрі, що забезпечує їх захист та можливість перевірки достовірності без централізованого посередника. Дослідження у цій галузі зосереджуються на інтеграції SSI із сервісами охорони здоров'я, освіти, державного управління, де ідентифікація є ключовою функцією [9].

Разом з тим, у літературі акцентується увага на технічних та етичних обмеженнях, зокрема складності дотримання норм конфіденційності, таких як GDPR, при зберіганні персональних даних у незмінних блокчейн-структурах [10]. Частина дослідників пропонує використання гібридних моделей, у яких конфіденційні дані зберігаються поза реєстром, а у самому блокчейні зберігаються лише хеші чи маркери верифікації [11].

Незважаючи на значну кількість досліджень, досі залишається відкритим питання практичної реалізації масштабованої та безпечної моделі, що дозволяє поєднати прозорість, контроль користувача, відповідність нормативним вимогам та ефективність обробки. Це зумовлює необхідність формування нових підходів до організації сховищ персональних даних на основі розподілених реєстрів, з урахуванням особливостей сучасних цифрових сервісів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Запропонована система зберігання та верифікації персональних даних ґрунтується на поєднанні технологій розподіленого реєстру, криптографічного захисту та децентралізованого контролю доступу. Основна ідея полягає в тому, щоб перенести довіру від централізованих органів до алгоритмічно забезпеченої моделі, де дані захищено, їх зміну можна простежити, а верифікацію здійснюють незалежні вузли без порушення конфіденційності.

Функціонально система складається з кількох взаємопов'язаних модулів: модуль збору персональних даних, що реалізує первинне введення та попередню обробку; модуль шифрування, який виконує криптографічне перетворення чутливих даних із використанням алгоритмів симетричного шифрування та створює геш-ідентифікатори; модуль формування блоку для запису в розподілений реєстр; модуль керування доступом, що реалізує смарт-контракти для визначення прав користувачів; модуль верифікації, який забезпечує перевірку автентичності та цілісності записів.

Узагальнена схема демонструє потік даних від моменту введення до моменту верифікації. Користувач передає дані, які обробляються шифрувальним модулем. Зашифрована частина зберігається у захищеному сховищі, а метадані (у вигляді гешів, ідентифікаторів та часових міток) формують блок, який записується до розподіленого реєстру. Модуль смарт-контрактів фіксує правила доступу до конкретних частин даних, а модуль верифікації дозволяє за запитом перевірити достовірність і цілісність запису без розкриття його вмісту.

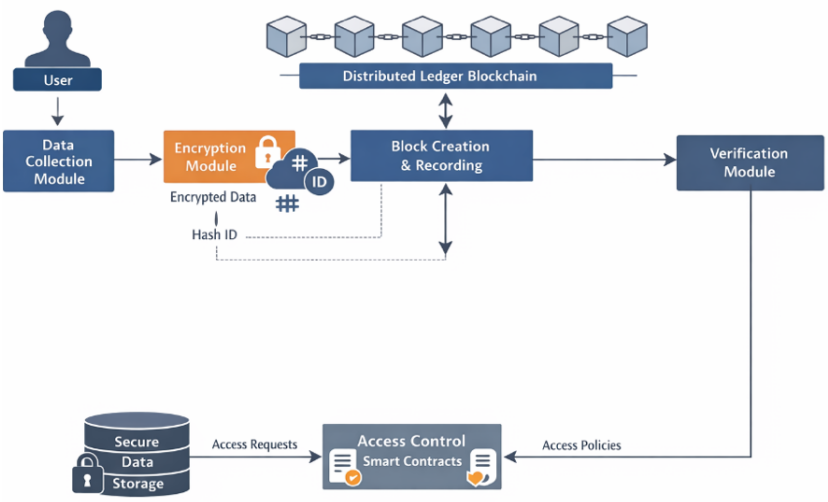

Рис. 1. Архітектура системи зберігання та верифікації персональних даних на основі розподіленого реєстру

Для запису інформації в розподілений реєстр формується стандартизований блок даних, структура якого забезпечує прозорість, захищеність і зручність подальшої перевірки. Кожен блок містить такі елементи: унікальний ідентифікатор запису (Record_ID), публічний ключ користувача або органу, що створив запис (PubKey), геш зашифрованого повідомлення (Hash_Data), часову мітку (Timestamp), посилання на попередній блок (Prev_Hash), а також смарт-контракт або посилання на нього (Access_Policy).

Специфіка моделі передбачає поділ даних на публічну та конфіденційну частини. У розподілений реєстр потрапляє лише обмежений набір метаданих, який не дозволяє ідентифікувати особу без відповідного ключа. Основна конфіденційна інформація шифрується й зберігається у відповідному зашифрованому середовищі, доступ до якого регулюється через смарт-контракти.

Таблиця 1

Формат запису у блок реєстру

Поле	Опис
Record_ID	Унікальний ідентифікатор запису
PubKey	Публічний ключ автора запису
Hash_Data	Геш зашифрованих персональних даних
Timestamp	Час створення запису
Prev_Hash	Посилання на хеш попереднього блоку
Access_Policy	Ідентифікатор або вміст смарт-контракту доступу

Подана структура дозволяє відокремити механізм перевірки достовірності від фактичного вмісту даних, забезпечуючи високий рівень конфіденційності без шкоди для прозорості верифікаційного процесу.

Механізм криптографічного захисту та контролю доступу ґрунтується на поєднанні симетричних і асиметричних криптографічних алгоритмів, що забезпечують цілісність, автентичність та конфіденційність персональних даних. Для шифрування вмісту персональних даних застосовуються сучасні симетричні алгоритми з високою ефективністю, зокрема AES із ключами змінної довжини, адаптованими до обмежених обчислювальних ресурсів. Для забезпечення автентичності використовується алгоритм цифрового підпису, наприклад ECDSA, що дозволяє підтвердити, що запис у реєстрі створений саме авторизованим суб'єктом.

Управління ключами є критичним елементом системи. Запропонована модель підтримує мультипідпис (multisignature scheme), за якого доступ до конфіденційних даних надається лише за наявності підтвердження від кількох довірених сторін. Наприклад, для розшифрування даних пацієнта в медичній системі може знадобитися підпис як самого пацієнта, так і лікаря, що підвищує безпеку та дозволяє реалізувати децентралізовану політику прийняття рішень. Як альтернативу можна використовувати модель розділених ключів (threshold scheme), за якої ключ доступу до даних розподіляється між кількома учасниками, і його відновлення можливе лише за умови згоди більшості.

Контроль доступу до персональних даних реалізується за допомогою смарт-контрактів, які містять правила авторизації, ролі користувачів, обмеження за часом, частотою доступу тощо. Смарт-контракт автоматично перевіряє права доступу під час кожного запиту до системи й приймає рішення про дозвіл чи відмову без участі людського фактора. Політика доступу може бути записана у вигляді логічних умов або таблиць відповідностей, що оновлюються в разі зміни статусу користувача чи організації.

Модель розмежування прав доступу формалізується у вигляді матриці доступу, де стовпці відповідають типам суб'єктів (користувач, адміністратор, лікар, нотаріус тощо), а рядки – типам операцій (перегляд, редагування, верифікація, запит). Наприклад, лікар може мати право лише на перегляд певної групи

даних, тоді як сам користувач має повний контроль. Ця матриця може динамічно змінюватися відповідно до ролей і прав, визначених у смарт-контракті.

Алгоритм верифікації даних побудований з урахуванням потреби перевірки достовірності записів без розкриття їхнього змісту. Процес перевірки починається з отримання запиту на верифікацію, після чого система використовує хеш ID, записаний у блокчейні, для зіставлення з обчисленим хешем даних, що зберігаються у зашифрованому вигляді. Якщо хеші збігаються, це гарантує, що дані не змінювалися з моменту створення запису. Для забезпечення конфіденційності при верифікації може використовуватись підхід zero-knowledge proof (ZKP), який дозволяє довести правильність даних без їх розкриття [12].

На рис. 2 показано послідовність: формування запиту на верифікацію, ідентифікація запису в реєстрі, обчислення хешу зі сторони запитувача, порівняння з хешем у реєстрі, прийняття рішення про достовірність.

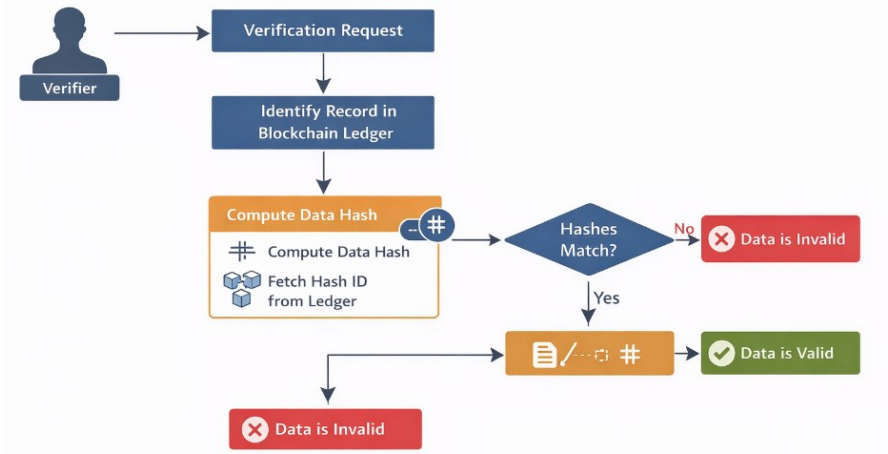

Рис. 2. Алгоритмічна схема процесу верифікації персональних даних у системі з використанням блокчейн-записів

Оцінка ефективності механізму верифікації проводилась з урахуванням часу відповіді системи та обчислювального навантаження на вузли. У типовому середовищі тестування (на основі емулятора блокчейну Hyperledger Fabric) час верифікації одного запису становив у середньому 120–180 мс при обсязі метаданих до 1 КБ. Споживання ресурсів було мінімальним завдяки використанню попередньо обчислених хешів і відсутності потреби у доступі до повного вмісту зашифрованих даних. Це дозволяє масштабувати систему без суттєвого зростання навантаження.

Інтеграція запропонованої моделі зберігання та верифікації персональних даних із зовнішніми цифровими сервісами реалізується через стандартні API-інтерфейси, які дозволяють здійснювати запити на запис, верифікацію, а також контроль доступу до даних. API підтримує REST-архітектуру та JSON-формат обміну, що забезпечує сумісність із більшістю сучасних веб-сервісів та мобільних застосунків. Для автентифікації запитів використовується система токенів доступу (наприклад, JWT) з підписом на основі відкритого ключа.

Механізм взаємодії з існуючими цифровими платформами побудований на концепції взаємодії через проксі-шлюзи, які адаптують запити з боку зовнішньої системи до специфікацій внутрішнього API. Це дозволяє легко підключати модель до платформ електронного врядування, де необхідно підтверджувати автентичність поданих документів, а також до банківських сервісів для перевірки персоніфікованої інформації. Наприклад, під час подання заявки на кредит, банк може здійснити запит на верифікацію задекларованих даних клієнта, не маючи прямого доступу до їхнього змісту.

Серед типових сценаріїв використання моделі можна виокремити: перевірку дипломів і сертифікатів при подачі до навчальних закладів або роботодавця; верифікацію медичних записів без передачі їх вмісту між установами; підтвердження електронної ідентичності користувача під час голосування або доступу до державних послуг; перевірку історії змін юридичних документів.

Експериментальна оцінка ефективності моделі проводилася у тестовому середовищі з використанням платформи Hyperledger Fabric 2.5 з емульованою мережею з 5 вузлів. Для вимірювання параметрів були використані стандартні інструменти Fabric CA та Chaincode Benchmarking Suite. Тестування охоплювало операції створення записів, верифікації, виконання смарт-контрактів і керування доступом. На рис. 3 представлено графіки залежності основних експлуатаційних показників, отриманих у процесі експериментального тестування в емуляційному середовищі.

Графіки результатів показали, що середній час створення одного запису в реєстрі становив 220 мс, що включає етап шифрування та обчислення гешу. Швидкість верифікації – від 100 до 180 мс залежно від розміру даних. Пам'яті для зберігання одного запису з метаданими достатньо в межах 1–2 КБ. Всі операції тестувалися на обладнанні із середніми характеристиками (4 CPU, 8 GB RAM, SSD-диск), що підтверджує придатність моделі для впровадження в умовах обмежених ресурсів.

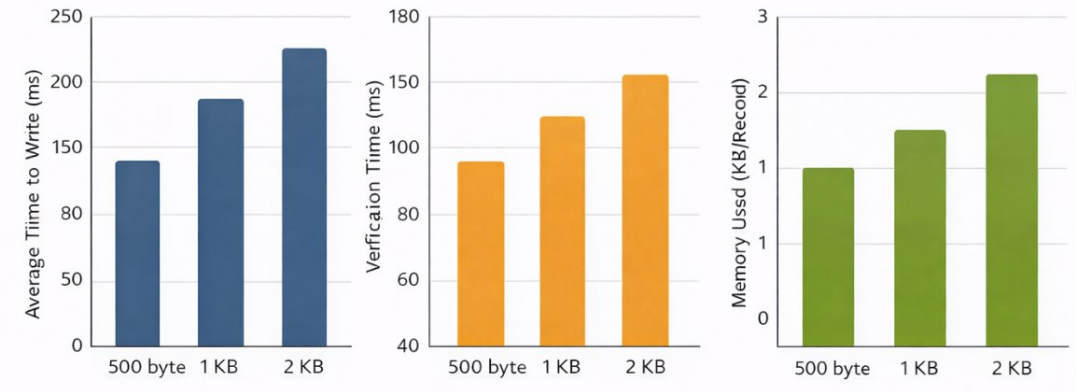

Рис. 3. Показники продуктивності запропонованої моделі зберігання та верифікації персональних даних на основі розподіленого реєстру

Для оцінки переваг запропонованої моделі було проведено порівняння з двома існуючими рішеннями: централізованим сховищем із традиційним контролем доступу та гібридною моделлю, в якій дані зберігаються в хмарі, а ідентифікатори – у блокчейні, табл. 2.

Таблиця 2

Порівняння характеристик запропонованої моделі та аналогів

Параметр	**Централізована система**	**Гібридна модель**	**Запропонована модель**
Цілісність даних	Середня	Висока	Висока
Прозорість доступу	Низька	Середня	Висока
Підтримка ZKP	Відсутня	Обмежена	Присутня
Автоматизований контроль доступу	Частково реалізований	Через зовнішні сервіси	Смарт-контракти
Ресурсоємність	Низька	Середня	Помірна
Підтримка мультипідпису	Відсутня	Обмежена	Повна

Результати підтверджують доцільність впровадження запропонованої моделі в умовах підвищених вимог до прозорості, децентралізації та довіри.

Запропонована модель зберігання та верифікації персональних даних має низку переваг порівняно з існуючими підходами. На відміну від централізованих систем, де повна відповідальність за збереження та обробку даних покладається на єдину організацію, розподілений підхід дозволяє уникнути єдиної точки відмови та мінімізувати ризики внутрішніх зловживань. У порівнянні з гібридними рішеннями, модель забезпечує вищу прозорість перевірок, автоматизоване керування доступом і вбудовану підтримку конфіденційності завдяки механізмам ZKP та мультипідпису. Інтеграція смарт-контрактів дозволяє гнучко визначати політики доступу, що легко адаптуються до змін нормативного середовища та особливостей конкретної галузі.

Модель має високий потенціал застосування в реальних цифрових системах, зокрема в державному секторі, охороні здоров'я, банківських і освітніх сервісах. В умовах зростаючих вимог до прозорості обробки персональних даних, запропоноване рішення може слугувати основою для побудови довірених платформ електронної ідентифікації, зберігання медичних записів, реєстрів населення, систем електронного голосування. Завдяки модульності архітектури та підтримці API, модель легко інтегрується з наявними сервісами, знижуючи бар'єри до впровадження.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У цій статті було запропоновано концептуальну та технологічну модель системи зберігання і верифікації персональних даних на основі розподіленого реєстру, що спрямована на усунення недоліків централізованих рішень, зниження ризиків несанкціонованого доступу до даних та підвищення довіри користувачів до цифрових платформ. Архітектура системи поєднує в собі модулі збору, шифрування, запису в блокчейн, управління доступом через смарт-контракти та перевірки достовірності інформації.

Було розроблено формат блоків для запису у розподілений реєстр, який дозволяє зберігати лише метадані у відкритому доступі, зберігаючи при цьому конфіденційність вмісту завдяки криптографічному захисту. Застосовано ефективні методи контролю доступу на основі мультипідпису та логіки розмежування прав у смарт-контрактах. Запропоновано алгоритм верифікації даних без їх розкриття з використанням хешування та підходів на кшталт zero-knowledge proof.

Результати експериментального дослідження продемонстрували низьке ресурсне навантаження системи, високу швидкість обробки запитів, стабільність при масштабуванні та придатність до впровадження

в системах з обмеженими обчислювальними ресурсами. Проведено порівняльний аналіз із наявними підходами, який підтвердив переваги запропонованої моделі за показниками прозорості, гнучкості керування доступом, відповідності сучасним підходам до захисту приватності.

Наукова новизна дослідження полягає у формалізації цілісної децентралізованої моделі керування персональними даними, яка поєднує технології блокчейн, криптографію та програмовану логіку доступу. Модель може стати основою для створення національних або галузевих довірених цифрових інфраструктур, зокрема в електронному врядуванні, охороні здоров'я, фінансовій та освітній сферах.

Подальші дослідження передбачають розширення функціоналу системи в частині:

- реалізації міжреєстрової взаємодії для підтримки інтеграції з іншими блокчейн-мережами;
- адаптації моделі до нормативних вимог різних країн, зокрема імплементації принципів GDPR;
- створення програмного прототипу та його тестування в умовах реального навантаження;
- удосконалення політик доступу за допомогою технологій машинного навчання для динамічного управління правами користувачів;
- дослідження аспектів енергоефективності та оптимізації криптографічних процедур для пристроїв з обмеженими ресурсами.

Запропонована модель є перспективною платформою для розбудови нових типів цифрових сервісів, де довіра користувачів базується не лише на інституційних гарантіях, а й на прозорій та захищеній технологічній основі.

Література

1. Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. *Management Science*, 69(8), 4389–4412. https://doi.org/10.1287/mnsc.2022.4514
2. Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, 12(4), 1927. https://doi.org/10.3390/app12041927
3. Zhu, R., Wang, M., Zhang, X., & Peng, X. (2023). Investigation of personal data protection mechanism based on blockchain technology. *Scientific Reports*, 13(1), 21918. https://doi.org/10.1038/s41598-023-49057-0
4. Vignesh Saravanan, K., Jothi Thilaga, P., Kavipriya, S., & Vijayalakshmi, K. (2023). Data protection and security enhancement in cyber-physical systems using AI and blockchain. In *AI Models for Blockchain-Based Intelligent Networks in IoT Systems* (pp. 285–325). Springer. https://doi.org/10.1007/978-3-031-15098-2_11
5. Khanum, S., & Mustafa, K. (2023). A systematic literature review on sensitive data protection in blockchain applications. *Concurrency and Computation: Practice and Experience*, 35(1), e7422. https://doi.org/10.1002/cpe.7422
6. Daudén-Esmel, C., Castellà-Roca, J., & Viejo, A. (2024). Blockchain-based access control system for efficient and GDPR-compliant personal data management. *Computer Communications*, 214, 67–87. https://doi.org/10.1016/j.comcom.2023.11.020
7. Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, 22(15), 5641. https://doi.org/10.3390/s22155641
8. Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*, 2(2), 18. https://doi.org/10.1007/s44206-023-00041-y
9. Holovatskiy, N. T. (2024). Legal regulation of personal data protection: GDPR and the legislation of the USA, Canada, and Ukraine. *Uzhhorod National University Herald. Series: Law*, 2(85), 288–292.
10. Mukta, R., Paik, H. Y., Lu, Q., & Kanhere, S. S. (2022). A survey of data minimisation techniques in blockchain-based healthcare. *Computer Networks*, 205, 108766. https://doi.org/10.1016/j.comnet.2022.108766
11. Aad, I. (2023). Zero-knowledge proof. In *Trends in Data Protection and Encryption Technologies* (pp. 25–30). https://doi.org/10.1007/978-3-031-25618-9_3

References

1. Ke, T. T., & Sudhir, K. (2023). Privacy rights and data security: GDPR and personal data markets. *Management Science*, 69(8), 4389–4412. https://doi.org/10.1287/mnsc.2022.4514
2. Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, 12(4), 1927. https://doi.org/10.3390/app12041927
3. Zhu, R., Wang, M., Zhang, X., & Peng, X. (2023). Investigation of personal data protection mechanism based on blockchain technology. *Scientific Reports*, 13(1), 21918. https://doi.org/10.1038/s41598-023-49057-0
4. Vignesh Saravanan, K., Jothi Thilaga, P., Kavipriya, S., & Vijayalakshmi, K. (2023). Data protection and security enhancement in cyber-physical systems using AI and blockchain. In *AI Models for Blockchain-Based Intelligent Networks in IoT Systems* (pp. 285–325). Springer. https://doi.org/10.1007/978-3-031-15098-2_11
5. Khanum, S., & Mustafa, K. (2023). A systematic literature review on sensitive data protection in blockchain applications. *Concurrency and Computation: Practice and Experience*, 35(1), e7422. https://doi.org/10.1002/cpe.7422
6. Daudén-Esmel, C., Castellà-Roca, J., & Viejo, A. (2024). Blockchain-based access control system for efficient and GDPR-compliant personal data management. *Computer Communications*, 214, 67–87. https://doi.org/10.1016/j.comcom.2023.11.020

7. Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, 22(15), 5641. https://doi.org/10.3390/s22155641
8. Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. *Digital Society*, 2(2), 18. https://doi.org/10.1007/s44206-023-00041-y
9. Holovatskiy, N. T. (2024). Legal regulation of personal data protection: GDPR and the legislation of the USA, Canada, and Ukraine. *Uzhhorod National University Herald. Series: Law*, 2(85), 288–292.
10. Mukta, R., Paik, H. Y., Lu, Q., & Kanhere, S. S. (2022). A survey of data minimisation techniques in blockchain-based healthcare. *Computer Networks*, 205, 108766. https://doi.org/10.1016/j.comnet.2022.108766
11. Aad, I. (2023). Zero-knowledge proof. In *Trends in Data Protection and Encryption Technologies* (pp. 25–30). https://doi.org/10.1007/978-3-031-25618-9_3