**COMPUTER SYSTEMS AND NETWORKS**

**Vol. 7, No. 1, 2025**

DOI: https://doi.org/10.23939/csn2025.01.001

**УДК 004.056.5**

# РОЗРОБКА МЕТОДУ ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ТА БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У БЛОКЧЕЙН-СИСТЕМАХ ДЕРЖАВНИХ РЕЄСТРІВ

**В.С. Балацька [1,2], В.О. Побережник [2], А.В. Стефанків [2], Ю.А. Шевчук [2,3]**

[1]Львівський державний університет безпеки життєдіяльності,
кафедра управління інформаційною безпекою
[2]Національний університет "Львівська політехніка",
кафедра захисту інформації
[3]DataArt, Northbrook, Illinois, USA
*E-mail: v.balatska@ldubgd.edu.ua, valeriia.s.balatska@lpnu.ua, , vasyl.poberezhnyk@gmail.com, artem.stefankiv.mkbas.2024@lpnu.ua, shev4ukyuri@gmail.com*



**У статті розглянуто проблему забезпечення достовірності та безпеки персональних даних, що обробляються у державних реєстрах, шляхом використання блокчейн-технологій. Зростання вимог до прозорості та стійкості державних систем управління даними висуває нові виклики щодо захисту інформації від несанкціонованих змін, втручань та підробок. Запропоновано метод, що базується на впровадженні децентралізованої блокчейн-архітектури для забезпечення цілісності даних, їх відстежуваності та прозорості у процесі обробки й зберігання.**

**Основою розробленого методу є використання розподіленого реєстру, який забезпечує незмінність внесеної інформації завдяки механізму ланцюгів блоків, що пов'язують транзакції та зміни у даних в хронологічному порядку. Смарт-контракти використовуються для автоматизації процесів внесення, оновлення та перевірки даних у державних реєстрах, що знижує ймовірність людського фактора та забезпечує довіру між усіма учасниками системи.**

**Запропонований метод дає змогу підвищити стійкість державних реєстрів до зовнішніх загроз, внутрішніх помилок та несанкціонованих змін завдяки прозорості та децентралізації, властивим блокчейн-технологіям. Практична реалізація методу продемонструвала покращення рівня безпеки персональних даних та ефективності функціонування реєстраційних систем на прикладі моделювання блокчейн-реєстру.**

**Ключові слова: блокчейн, достовірність даних, державні реєстри, децентралізація, безпека інформації, смарт-контракти, розподілений реєстр.**

## Вступ

Забезпечення достовірності та безпеки персональних даних є надзвичайно важливим завданням у процесі цифровізації державного управління. Державні реєстри відіграють ключову роль у наданні публічних послуг, здійсненні адміністративного контролю та реалізації прав громадян. Вони містять критично важливу інформацію про фізичних та юридичних осіб, що використовується у сферах правосуддя, соціального захисту, економічного регулювання та інших адміністративних

процесах. Проте централізовані системи управління даними мають суттєві недоліки, які знижують їх ефективність і надійність. Одним із головних ризиків є можливість несанкціонованих змін або маніпуляцій із записами, що може призвести до серйозних юридичних наслідків. Вразливість до кібератак, технічних збоїв і внутрішніх помилок також ставить під загрозу цілісність інформації, особливо коли йдеться про державні бази даних, які часто стають об'єктами хакерських атак.

Зростаюча кількість інцидентів із компрометацією державних інформаційних систем підтверджує критичність цієї проблеми. Наприклад, у грудні 2024 року в Україні відбулася масштабна атака на державні реєстри, внаслідок якої хакери отримали доступ до конфіденційних даних та спричинили тимчасове порушення роботи ключових інформаційних систем. Цей інцидент вкотре продемонстрував вразливість централізованих реєстрів до кібератак і необхідність переходу до більш стійких технологічних рішень. Подібні випадки траплялися і раніше, зокрема у 2021 році стався витік даних із державного реєстру України, що призвів до розголошення персональної інформації тисяч громадян [1]. У США у 2020 році хакери здійснили атаку на систему реєстрації нерухомості, внаслідок чого були внесені неправомірні зміни до записів [2]. Такі події вказують на системні проблеми у сфері безпеки державних інформаційних ресурсів і підтверджують необхідність пошуку нових підходів до забезпечення їхньої стійкості.

Одним із головних викликів, що супроводжують роботу державних реєстрів, є обмежена прозорість процесів внесення та оновлення даних. У традиційних централізованих системах аудит змін може бути складним і трудомістким процесом, оскільки доступ до історії записів часто обмежений. Це створює ризики як для громадян, які можуть стати жертвами неправомірних змін у реєстрах, так і для державних органів, яким необхідно забезпечити контроль за достовірністю даних. Людський фактор залишається додатковим джерелом загроз, оскільки будь-яка система, що залежить від ручного введення інформації, є вразливою до помилок або навмисного викривлення даних. В умовах швидкої цифрової трансформації та зростаючої залежності державних установ від інформаційних технологій пошук ефективних рішень для захисту персональних даних та забезпечення надійності реєстрів стає критично важливим завданням.

На тлі цих викликів блокчейн-технології стають перспективним інструментом, здатним забезпечити прозорість, незмінність та безпеку державних реєстрів. Децентралізована структура блокчейну унеможливлює одноосібний контроль над даними, оскільки вони розподіляються між вузлами мережі, що робить їх стійкими до збоїв і атак. Використання криптографічних алгоритмів гарантує незмінність записів, оскільки кожна транзакція додається у блок, який зберігає унікальний хеш попередніх даних, унеможливлюючи підробку чи несанкціоноване видалення інформації [3]. Прозорість блокчейн-реєстрів забезпечується механізмом публічного аудиту, що дає змогу перевіряти всі зміни та транзакції без ризику втручання. Крім того, автоматизація процесів через смарт-контракти дозволяє значно зменшити вплив людського фактора, оскільки вони забезпечують виконання операцій виключно за заздалегідь визначеними правилами [4].

Застосування блокчейн-технологій у сфері державного управління вже привернуло увагу багатьох країн. Естонія успішно використовує блокчейн для захисту державних реєстрів, зокрема у системі цифрової ідентифікації громадян, що дає змогу забезпечити довіру до державних сервісів і зменшити ризики шахрайства. У Грузії технологію було інтегровано в систему реєстрації нерухомості, що дозволило створити незмінний цифровий слід усіх транзакцій, підвищуючи довіру до операцій купівлі-продажу [5]. В інших країнах тривають експерименти щодо впровадження блокчейн-рішень у державні системи голосування, податкові служби та системи соціального забезпечення, що свідчить про зростаюче визнання потенціалу цієї технології для державного сектору.

Незважаючи на значні переваги, блокчейн-технології все ще стикаються з викликами під час впровадження. Однією з основних проблем є інтеграція з наявними інформаційними системами, що потребує адаптації інфраструктури та зміни підходів до зберігання і обробки даних. Питання масштабованості також залишається актуальним, оскільки традиційні блокчейн-мережі, такі як

Bitcoin чи Ethereum, обмежені у швидкості обробки транзакцій [6]. Крім того, необхідно розробити механізми ідентифікації користувачів і управління правами доступу, оскільки державні реєстри містять чутливі дані, що не можуть бути повністю відкритими для всіх учасників мережі.

Попри ці виклики, розвиток блокчейн-рішень триває, а дослідження спрямовані на вдосконалення механізмів масштабування, підвищення ефективності та створення нових моделей управління доступом до даних. Враховуючи актуальні проблеми, пов'язані із захистом державних реєстрів, використання блокчейн-технологій може стати фундаментальним кроком до створення більш безпечних, прозорих і ефективних систем управління персональними даними.

## Огляд літературних джерел

Сучасні державні реєстри є важливим інструментом для управління інформацією, що стосується громадян, юридичних осіб та їхніх активів. Вони забезпечують реалізацію ключових адміністративних функцій, надання державних послуг та підтримку правової системи. Однак зростання обсягів даних та їх обробки супроводжується численними викликами у контексті достовірності, безпеки та прозорості інформації.

Централізована архітектура державних реєстрів є одним із головних недоліків традиційних систем. Вона передбачає збереження даних у єдиному сховищі, що створює ризик їх несанкціонованої модифікації або втрати через технічні збої чи атаки. Подібна вразливість призводить до ситуацій, коли зміни у реєстрах залишаються непоміченими або не можуть бути відстежені, що ставить під загрозу достовірність даних, особливо у критично важливих системах [7].

Ще однією проблемою є низька прозорість процесів внесення та оновлення даних. Відсутність ефективного контролю у централізованих системах дозволяє зловмисникам або внутрішнім працівникам вносити некоректну інформацію без належного аудиту [8]. Це призводить до фінансових збитків, юридичних суперечок та втрати довіри громадян до державних інституцій.

Людський фактор залишається одним із ключових джерел загроз для централізованих систем. Ручне внесення даних, помилки операторів та зловмисні дії значно підвищують ризик компрометації інформації. При цьому слабкі механізми валідації внесених даних роблять такі системи уразливими до неправомірних змін, що особливо небезпечно для державних реєстрів.

Зазначені проблеми загострюються у контексті сучасних кіберзагроз. Атаки на державні інформаційні системи зростають як у кількісному, так і в якісному аспектах. Зокрема, технології фішингу, соціальної інженерії та прямі атаки на бази даних стають дедалі витонченішими, що потребує підвищення рівня захисту таких систем [9].

У цьому контексті перспективним рішенням є застосування блокчейн-технологій. Блокчейн забезпечує незмінність даних завдяки децентралізованій структурі та механізму ланцюгів блоків, де кожна транзакція записується у хронологічному порядку. Це дає змогу вирішити проблему контролю внесення інформації, забезпечуючи можливість аудиту та відстеження всіх змін. Дослідження підтверджують, що використання блокчейн може значно підвищити рівень довіри до державних реєстрів завдяки прозорості їх функціонування та стійкості до несанкціонованих змін.

Отже, виклики, пов'язані з централізованими системами державних реєстрів, зумовлюють необхідність розробки інноваційних рішень, які забезпечать їх достовірність, безпеку та прозорість. Застосування блокчейн-технологій є одним із перспективних напрямів, що дає змогу модернізувати наявні системи та підвищити їх стійкість до сучасних загроз.

## Постановка задачі

Сучасні державні реєстри стикаються з низкою проблем, які знижують їх ефективність та надійність. Центральна архітектура таких систем є вразливою до технічних збоїв, кібератак та несанкціонованих змін даних. Відсутність прозорості процесів внесення та оновлення інформації створює ризики для маніпуляцій, а людський фактор часто стає причиною помилок або свідомого

втручання. Ці недоліки підривають довіру до державних реєстрів як інструменту збереження критично важливих даних громадян і організацій.

Водночас блокчейн-технології дають змогу створити систему, яка забезпечить незмінність, прозорість та надійність обробки даних. Завдяки децентралізованому зберіганню інформації кожна операція може бути зафіксована у вигляді незмінного запису, а хронологічний ланцюг блоків гарантує неможливість внесення несанкціонованих змін [6]. Автоматизовані механізми валідації даних, вбудовані в блокчейн, мінімізують вплив людського фактора та підвищують стійкість системи до внутрішніх і зовнішніх загроз.

Отож постає завдання розробити метод, який забезпечить достовірність та безпеку персональних даних у державних реєстрах шляхом впровадження блокчейн-технологій. Розробка такого методу має враховувати особливості функціонування державних реєстраційних систем, забезпечувати прозорий контроль над операціями та підвищувати стійкість до сучасних викликів цифрової безпеки.

**Мета статті** полягає у розробці методу забезпечення достовірності та безпеки персональних даних на основі блокчейн-технологій, що сприятиме підвищенню прозорості, стійкості та надійності державних реєстрів.

**Завдання:**

1) дослідити основні виклики та проблеми, пов’язані з безпекою та достовірністю персональних даних у сучасних державних реєстрах;

2) проаналізувати можливості застосування блокчейн-технологій для підвищення надійності та прозорості реєстрів;

3) розробити метод забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів.

Обґрунтувати ефективність запропонованого методу на основі аналізу його переваг порівняно з традиційними методами забезпечення достовірності та безпеки даних у державних реєстрах.

## Потенціал блокчейн-технологій для підвищення достовірності та безпеки даних у державних реєстрах

Блокчейн-технології є інноваційним рішенням для вирішення проблем, пов’язаних із забезпеченням достовірності, безпеки та прозорості державних реєстрів. Основною перевагою блокчейну є його децентралізована архітектура, що усуває залежність від центрального сховища даних. Інформація у блокчейн-системах записується у вигляді послідовних блоків, які пов’язані між собою криптографічними хешами. Це забезпечує незмінність даних і унеможливлює їх несанкціоновану модифікацію або видалення [10].

У традиційних державних реєстрах дані зберігаються у централізованих сховищах, що створює ризик компрометації через атаки або помилки у системі. Використання блокчейну дає змогу розподілити копії реєстру між вузлами мережі, забезпечуючи надійність та стійкість до збоїв. Кожна операція записується у блок, який не може бути змінений без консенсусу всієї мережі. Це робить блокчейн-системи стійкими до фальсифікації та маніпуляцій даними [11].

У блокчейн-системах кожна транзакція є доступною для перегляду учасниками мережі, що забезпечує повний контроль над внесеними змінами та підвищує прозорість роботи державних реєстрів. Завдяки цьому будь-які спроби несанкціонованого втручання або внесення помилкових даних можуть бути легко виявлені та усунені. Такий механізм є особливо важливим для державних установ, оскільки дозволяє забезпечити довіру громадян до інформації у реєстрах [12].

Автоматизація процесів валідації та внесення даних за допомогою блокчейн-смарт-контрактів дає змогу мінімізувати вплив людських помилок або свідомих маніпуляцій. Смарт-контракти є програмами, які автоматично виконують умови угоди між учасниками мережі. Це забезпечує

контрольоване внесення змін у державний реєстр лише за умови виконання заданих правил, що значно підвищує рівень безпеки [13].

Використання блокчейн-систем підвищує стійкість державних реєстрів до кібератак завдяки розподіленій структурі. Замість того, щоб атакувати єдину точку доступу, зловмиснику необхідно змінити всі копії реєстру на всіх вузлах мережі одночасно, що практично неможливо через обчислювальну складність.

Застосування блокчейн-технологій у державних реєстрах дає змогу обробляти великі обсяги даних з можливістю їх розширення в майбутньому. Розробка моделей, орієнтованих на швидкість транзакцій і оптимізацію зберігання, дозволяє адаптувати блокчейн до потреб державних систем управління [14].

Основні проблеми централізованих систем, такі як вразливість до атак, відсутність прозорості та залежність від людського фактора, можна вирішити за допомогою блокчейн-технологій. У табл. 1 наведено порівняння характеристик централізованих та блокчейн-систем у контексті вирішення цих викликів.

*Таблиця 1*

**Порівняльний аналіз блокчейн-технологій та традиційних методів управління державними реєстрами**

| Критерій | Традиційні централізовані системи | Блокчейн-системи |
|---|---|---|
| **Архітектура** | Централізована (єдина точка збереження даних) | Децентралізована (розподілений реєстр) |
| **Стійкість до збоїв та атак** | Низька: ризик атак на центральний сервер | Висока: зміни потребують консенсусу всіх вузлів |
| **Прозорість** | Обмежена: відсутність чіткого аудиту змін | Висока: всі зміни фіксуються та доступні для перевірки |
| **Незмінність даних** | Дані можна змінити або видалити | Незмінність завдяки ланцюговій структурі блоків |
| **Безпека** | Залежна від зовнішніх механізмів захисту | Вбудований захист через криптографію та консенсус |
| **Автоматизація процесів** | Обмежена: потребує людської перевірки | Висока: смарт-контракти автоматизують процеси |
| **Контроль внесення змін** | Низький: можливі помилки та маніпуляції | Високий: всі зміни валідуються мережею |
| **Витрати на підтримку** | Високі через централізовану інфраструктуру | Помірні: автоматизація знижує витрати |

З наведеного порівняльного аналізу видно, що блокчейн-системи значно перевершують традиційні централізовані рішення за ключовими показниками. Децентралізована архітектура забезпечує стійкість до атак і збоїв, а незмінність даних унеможливлює їх несанкціоновану модифікацію. Висока прозорість та можливість повного аудиту усіх змін підвищують довіру користувачів, що є особливо важливим для державних реєстрів.

Отже, впровадження блокчейн-технологій створює умови для забезпечення достовірності, прозорості та захисту державних реєстрів від сучасних загроз, усуваючи основні недоліки централізованих систем [15].

**Розробка методу забезпечення достовірності та безпеки персональних даних у державних реєстрах на основі блокчейн-технологій**

Запропонований метод забезпечення достовірності та безпеки персональних даних у державних реєстрах ґрунтується на блокчейн-технологіях. Його основна мета – створення системи, що забезпечує незмінність, прозорість та стійкість до загроз у процесі обробки та зберігання даних.

Ключовою ідеєю методу є розподілений реєстр блокчейн, у якому кожна операція фіксується у блоках, що зв’язуються між собою за допомогою криптографічних хешів. Це забезпечує:

1) незмінність даних: будь-які зміни залишають слід у системі;
2) прозорість: усі учасники мають доступ до записів у реєстрі для перевірки їх достовірності;
3) контроль доступу: система автоматично регулює внесення та оновлення даних на основі смарт-контрактів.

Архітектура запропонованого методу складається з чотирьох основних компонентів:

1. **Користувач (Data Submitter)**

Ініціює запити на внесення нових даних, оновлення існуючих записів або перегляд інформації у державному реєстрі.

2. **Модуль валідації (Validation Module)**

Перевіряє коректність запиту: синтаксис даних, права доступу користувача та дотримання правил внесення змін.

3.**Смарт-контракти (Smart Contracts)**

Автоматично контролюють умови виконання операцій. Дозволяють або блокують зміни залежно від заданих правил доступу.

4.**Блокчейн-реєстр (Blockchain Registry)**

Децентралізована база даних, у якій фіксуються всі підтверджені операції. Новий блок записується у реєстр після досягнення консенсусу вузлами мережі.

На рис. 1 наведено блок-схему роботи запропонованого методу, що відображає основні етапи взаємодії компонентів системи.

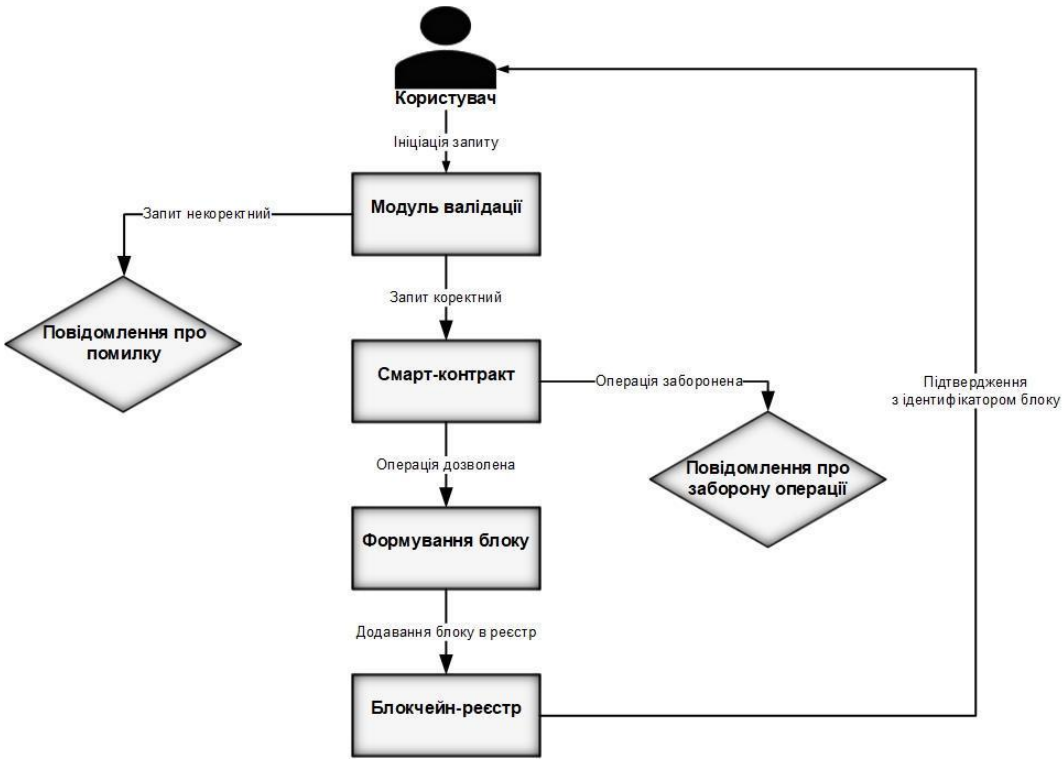


*Рис. 1. Блок-схема роботи методу забезпечення достовірності даних*

**Крок 1. Ініціація запиту**

Користувач надсилає запит на внесення, оновлення або перегляд даних через клієнтський інтерфейс системи.

**Крок 2. Валідація запиту**

Модуль валідації перевіряє:

- ідентифікацію користувача та його права доступу;
- коректність структури та змісту запиту;
- дотримання правил внесення даних у реєстр.

**Крок 3. Виконання смарт-контракту**

Після успішної валідації смарт-контракт автоматично перевіряє умови операції та, якщо всі критерії дотримані, формує новий блок для додавання у блокчейн-реєстр.

**Крок 4. Формування блоку**

Новий блок містить:

- хеш попереднього блоку для зв’язку у ланцюзі;
- часову мітку операції;
- дані про користувача та зміст операції;
- хеш-код транзакції як підтвердження цілісності даних.

**Крок 5. Запис у блокчейн-реєстр**

Після досягнення консенсусу блок додається у розподілений реєстр, де він стає доступним для перевірки всіма учасниками мережі.

**Крок 6. Аудит і підтвердження операції**

Користувач отримує підтвердження про успішну операцію з ідентифікатором нового блоку. Всі записи є доступними для аудиту та перевірки їх достовірності.

Рис. 1 наочно демонструє архітектуру методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Основою запропонованого підходу є розподілений блокчейн-реєстр, у якому кожна операція фіксується у формі незмінних блоків, що зв’язуються криптографічними хешами. Це забезпечує як технічну неможливість несанкціонованого внесення змін, так і прозорість системи для всіх учасників. У методі інтегровано автоматизовані модулі валідації та смарт-контракти, які регулюють внесення й оновлення даних відповідно до заданих правил доступу [16].

Запропонований алгоритм реалізації базується на чіткій взаємодії між ключовими компонентами системи: користувачами, модулем валідації, смарт-контрактами та блокчейн-реєстром. Користувач надсилає запит на внесення або оновлення даних, який проходить автоматичну перевірку модулем валідації. Смарт-контракти забезпечують контроль за виконанням умов операції, після чого формується новий блок. Після досягнення консенсусу вузлів блок додається до блокчейн-реєстру, де дані стають незмінними й доступними для подальшого аудиту.

Особливістю методу є його стійкість до зовнішніх загроз завдяки децентралізованій структурі, яка усуває ризик “єдиної точки відмови”. Прозорість операцій досягається через можливість аудиту будь-якого запису в реєстрі, що підвищує довіру користувачів. Крім того, автоматизація процесів, забезпечена смарт-контрактами, мінімізує вплив людського фактора, а розмежування прав доступу сприяє ефективному управлінню інформацією.

Отже, запропонований метод забезпечує надійний механізм контролю внесення, оновлення та перевірки даних у державних реєстрах, що підтверджується схемою на рис. 1. Його застосування дає змогу модернізувати традиційні реєстраційні системи, підвищити рівень достовірності даних, мінімізувати ризики маніпуляцій та забезпечити прозорість функціонування державних інформаційних систем.

**Результати дослідження**

Сучасні державні реєстри, що базуються на централізованих системах управління даними, стикаються з численними викликами, пов'язаними із забезпеченням достовірності, цілісності та безпеки інформації. Серед найпоширеніших проблем можна виділити вразливість до збоїв через єдину точку відмови, низький рівень прозорості процесів та залежність від людського фактора під час обробки даних. Окрім цього, централізовані реєстри є вразливими до внутрішніх загроз, оскільки адміністратори або інші уповноважені особи можуть здійснювати зміни без належної фіксації в історії операцій [17]. Аудит у таких системах є трудомістким процесом, що потребує залучення додаткових ресурсів і часу, що робить їх менш ефективними у динамічних умовах цифрової трансформації.

Запропонований метод забезпечення достовірності та безпеки даних на основі блокчейн-технологій є науково обґрунтованим рішенням, яке усуває недоліки традиційних систем завдяки застосуванню розподіленого реєстру, автоматизованих смарт-контрактів та криптографічного хешування. Його ключова особливість полягає у тому, що кожен запис у системі є незмінним, а всі зміни фіксуються у прозорій та доступній для перевірки формі. Саме це забезпечує фундаментальну достовірність і цілісність даних у реєстрах, що є критично важливим у сучасних умовах поширення цифрових загроз та інформаційних маніпуляцій.

Відмінність запропонованого методу від централізованих підходів полягає у його децентралізованій архітектурі, яка усуває проблему "єдиної точки відмови" та значно підвищує стійкість до зовнішніх і внутрішніх загроз. Дані у блокчейн-реєстрі зберігаються на розподілених вузлах мережі, а кожен новий блок інформації пов'язаний із попереднім через криптографічний хеш. Це унеможливлює несанкціоновані зміни, оскільки будь-яке втручання призведе до порушення цілісності всього ланцюга. Крім того, блокчейн забезпечує повну прозорість процесів, дозволяючи учасникам системи у реальному часі проводити аудит операцій та перевіряти їх достовірність. На відміну від централізованих систем, де перевірка змін потребує додаткових процедур, у блокчейн-системі кожна операція автоматично фіксується та стає доступною для аналізу.

Запровадження смарт-контрактів у запропонованому методі вирішує ще одну важливу проблему традиційних реєстрів – залежність від людського фактора під час обробки запитів. Смарт-контракти є автоматизованими алгоритмами, що забезпечують контроль за внесенням і оновленням даних відповідно до заданих умов. Це дає змогу не лише мінімізувати ризик помилок, а й пришвидшити обробку операцій, що є надзвичайно актуальним для державних систем, які щоденно працюють з великими обсягами інформації [18].

Ефективність запропонованого методу проявляється у забезпеченні незмінності даних, що критично важливо для реєстрів нерухомості, реєстрів громадян, виборчих систем та інших інформаційних баз, де точність і достовірність інформації визначають легітимність управлінських рішень. Наприклад, у реєстрі нерухомості кожна операція купівлі-продажу фіксується як незворотна транзакція, що усуває можливість шахрайства або підробки документів. У реєстрі юридичних осіб використання блокчейн-технологій забезпечує прозорість і довіру завдяки доступності історії змін, що сприяє ефективному контролю за діяльністю компаній та їхніх бенефіціарів.

Для підтвердження достовірності даних, отриманих із реєстру запропонованої моделі, можна скористатися принципом "доказу існування" даних, який полягає у тому, що конкретні дані існують у незмінному стані із моменту їх створення. Досягти цього можна через поєднання технологій, основаних на застосуванні принципу децентралізації та блокчейн.

У такому підході для збереження даних доцільно застосовувати технології, які відмінні від блокчейн, оскільки розмір даних негативно впливає на швидкодію мережі та вартість її підтримки, а його застосування є доцільним для збереження критичних даних, які повинні зберігатися у незмінному стані та не мають займати порівняно небагато місця. До даних такої категорії можна зарахувати відбитки даних. Тобто застосування цього принципу потребує розподілу для збереження даних і збереження доказу їхньої достовірності.

Шляхом забезпечення достовірності даних є використання криптографічного хешування, що дає змогу створити відбиток даних певного встановленого розміру, не зважаючи на об'єм вхідних даних, ба більше, застосування криптографічного хешування дозволяє забезпечити неможливість відтворення вхідних даних із отриманого хеш-коду, що дає змогу застосовувати такий механізм для обробки різних даних, зокрема тих, що підпадають під категорії: обмежений доступ, персональні дані, службова інформація тощо.

Також будь-яка зміна у даних буде призводити до цілковитої зміни самого результату через "лавинні зміни" [19], що практично унеможливлює будь-які несанкціоновані зміни даних, оскільки їх наявність буде призводити до зміни самого хеш-коду, що одразу свідчитиме про зміну даних.

Застосування технології IPFS обґрунтовується, зокрема, її децентралізованою природою, яка, з одного боку, запобігає існуванню користувачів з особливими правами в мережі, а з іншого – підвищує стійкість системи, оскільки видаляє із системи центральну точку вразливості, що дозволить функціонувати системі, навіть якщо частина вузлів вийде з ладу. Ще однією перевагою цієї технології є збереження даних у децентралізованому вигляді, що дає змогу зберігати їх у кількох різних вузлах мережі одночасно, що дозволяє підвищити швидкість доступу до інформації, обираючи найближчий вузол до користувача системи, а також забезпечити дублювання даних на різних вузлах, що забезпечуватиме збереження доступу до них, навіть якщо найближчий вузол до користувача буде недоступним.

Згадані можливості технологій дають змогу розглядати поєднання блокчейн та IPFS, як основу для системи, яка зможе зберігати, передавати та перевіряти дані на їхню достовірність та цілісність, що дає змогу розглядати таку основу, як основу для державного реєстру нового покоління.

На рис. 2 зображено структуру пропонованого реєстру.

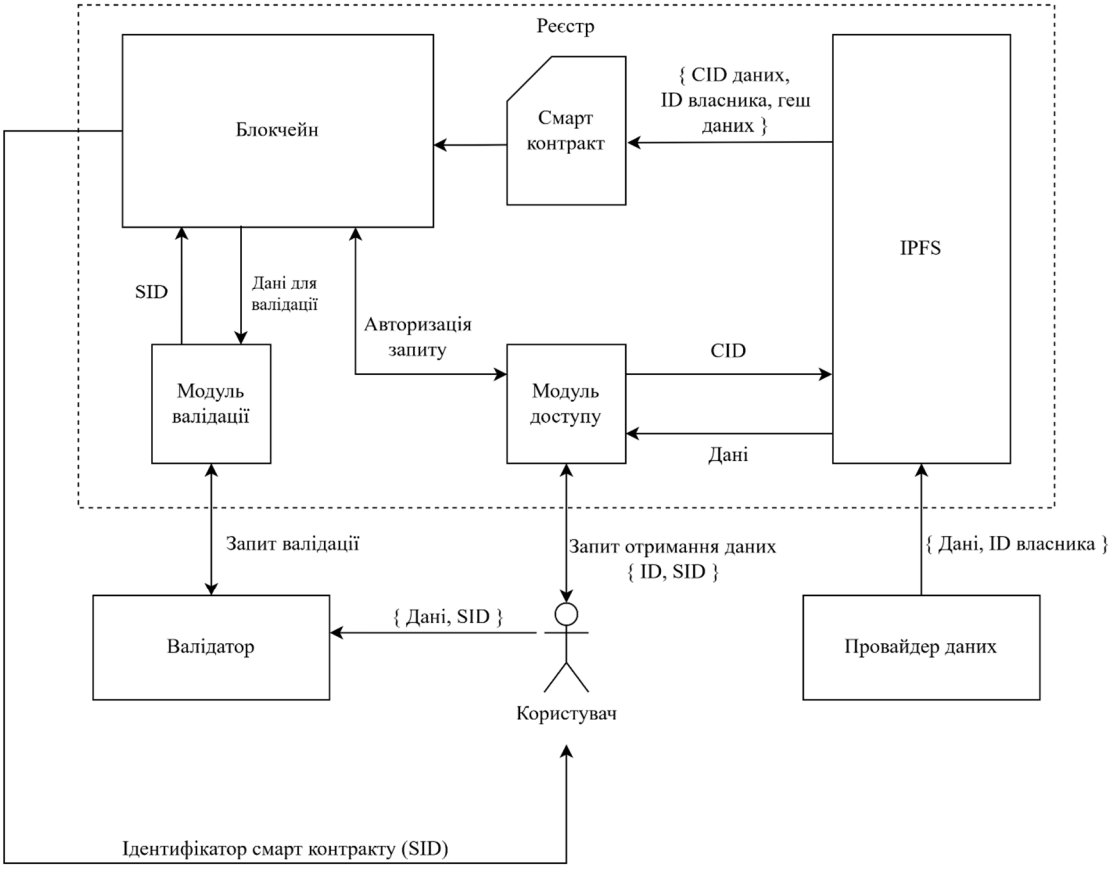


*Рис. 2. Структура пропонованого реєстру з використання блокчейн та IPFS*

У цій концепції кожна самостійна одиниця даних, наприклад сформований документ чи запис у реєстрі, постає у формі збереженого у блокчейн набору значень:

$$Entry = \{ SID,\ CID,\ ID,\ H \}, \quad (1)$$

де $Entry$ - запис у реєстрі; $SID$ - ідентифікатор смарт-контракту; $CID$ - ідентифікатор даних у IPFS; $ID$ - ідентифікатор власника; $H$ - хеш даних.

Окрім згаданих раніше технологій, в цій системі необхідно застосувати додаткові технології, зокрема смарт-контракти, які дають змогу автоматизувати роботу системи, що дозволить зменшити кількість людського втручання у систему, та одночасно підняти довіру до системи і мінімізувати кількість користувачів із особливими правами, які б могли негативно впливати на роботу системи чи вчиняти несанкціоновані дії. Ба більше, застосування смарт-контрактів дасть змогу автоматизувати не лише збереження чи перевірку даних, а й розмежувати доступ за потреби.

*Під час створення нового запису в реєстрі алгоритм додавання даних буде мати такий вигляд:*

1. Провайдер даних створює нові дані та передає їх та ідентифікатор власника даних (ID) у IPFS реєстру.
2. IPFS генерує ідентифікатор даних (CID) та криптографічний хеш даних і створює на основі цього смарт-контракт.
3. В смарт-контракті вказується CID, хеш даних та ідентифікатор власника.
4. Смарт-контракт зберігається у блокчейн частині реєстру та отримує ідентифікатор.
5. Користувач отримує ідентифікатор смарт-контракту та вважається його власником.
6. За необхідності користувач отримує дані з реєстру через модуль доступу, надаючи свій ідентифікатор та ідентифікатор смарт-контракту.

*Отримання доступу до даних користувачем матиме такі кроки:*

1. Користувач надсилає запит до модуля доступу, надаючи ID та SID.
2. Модуль доступу проводить автентифікацію запиту шляхом зіставлення отриманого ідентифікатора користувача та ідентифікатора користувача, який збережений у смарт-контракті, на який вказує SID.
3. Якщо ідентифікатори збігаються, то модуль доступу надсилає запит, який містить CID, до IPFS, якщо ідентифікатори не збігаються - відмовляє у доступі.
4. IPFS повертає вказані дані до модуля доступу, модуль доступу надсилає дані користувачу.

*Якщо є потреба перевірити отримані дані від користувача, процес валідації матиме такі кроки:*

1. Валідатор отримує дані та ідентифікатор смарт-контракту.
2. Валідатор обчислює криптографічний геш даних та надсилає запит валідації, який містить обчислений геш та ідентифікатор смарт-контракту.
3. Модуль валідації отримує із блокчейну дані для валідації із смарт-контракту, ідентифікатором якого є наданий SID.
4. Якщо обчислений геш та збережений у смарт-контракті геш збігаються, валідатор отримує відповідь про успішну валідацію, якщо геші не збігаються, - отримує повідомлення про помилку валідації, що може свідчити про порушення цілісності чи достовірності даних.

Однак застосування цих технологій може містити і негативні сторони, які найчастіше пов’язані із природою самих технологій, які застосовуються. Наприклад, розмір блокчейну буде негативно впливати на швидкодію всієї системи, оскільки з часом він ростиме, а швидкість обробки даних в мережі залежить від розміру блокчейн. Шляхом вирішення цього недоліку може стати “обнулення” блокчейну, коли інформація із старих блоків видаляється, а залишається тільки геш попереднього блоку, який дає змогу підтримувати ланцюжок у робочому стані, а повна версія блокчейн зберігається в архівних вузлах. Такий підхід буде знижувати рівень децентралізації в мережі, оскільки мережа матиме залежність від певної кількості архівних вузлів [20].

Іншим шляхом вирішення проблеми швидкодії та розміру блокчейн може стати застосування Layer 2 підходу. Суть якого полягає у тому, щоб обробляти дані поза блокчейн, а в ньому зберігати лише результат обробки. Наприклад, метод блокчейн-ролап дає змогу об'єднати кілька транзакцій, виконаних поза блокчейн в одну транзакцію, результат якої збережеться у блокчейн. Такий підхід дає змогу підвищити масштабованість та швидкодію блокчейн мережі.

Ще одним важливим елементом такого реєстру є механізм прийняття консенсусу, оскільки це фундаментальний процес, який відповідає за збереження даних у блокчейні. Під час роботи з державними реєстрами доцільним є застосувати алгоритм Proof of Authority. Відмінність полягає в тому, що він потребує наявності великих обчислювальних потужностей, як у Proof of Work, чи наявності певної кількості токенів, як у Proof of Stake. Цей алгоритм покладається на репутацію учасника мережі та довіру в мережі, які дають змогу обирати валідаторів мережі на основі певних характеристик, наприклад, репутація, внесок в розвиток мережі, стаж в мережі тощо. Такий алгоритм можна використовувати у приватних блокчейнах, де відомі усі учасники мережі чи мережах типу консорціум, де валідаторами виступають організації, які мають високий рівень довіри між собою. Через ці особливості такий алгоритм досягання консенсусу може стати відповідним варіантом для побудови реєстру, оскільки власник реєстру зможе наперед визначити валідаторів мережі, що є перевагою під час побудови державних реєстрів, оскільки убезпечить мережу від додавання невідомих вузлів. Однак такий алгоритм має ряд недоліків, які породжені його особливостями. У табл. 2 наведено переваги та недоліки запропонованого алгоритму.

Зважаючи на переваги та недоліки цього алгоритму консенсусу його використання в державних реєстрах може виявитися доцільним, оскільки держава чи безпосередні власник реєстру зможе керувати тим, хто може стати валідатором мережі. Такий підхід вносить певну відмову від повної децентралізації, однак дає змогу зберегти державі контроль над реєстром. Водночас може з'являтися певний рівень недовіри до мережі через можливість впливу на неї, проте таку ситуацію можна нівелювати збереженням коду смарт-контрактів та інших важливих елементів системи, у відкритому вигляді, щоб надати можливість користувачам такого реєстру впевнитися у доброчесності пропонованої системи.

*Таблиця 2*

**Переваги та недоліки алгоритму**

| Алгоритм | Переваги | Недоліки |
|---|---|---|
| **Proof of Authority** | – висока швидкодія: наперед визначених валідаторів не потребують складних обчислень;<br>– висока масштабованість: оскільки кількістю валідаторів можна керувати;<br>– енергоефективність: відсутність складних обчилень, як у PoW, призводить до менших затрат енергії | – зниження рівня децентралізації: обмежена кількість валідаторів керує мережею;<br>– ризик змови: у разі змови достатньої кількості вузлів вони можуть взяти мережу під контроль через порівняну невисоку загальну кількість валідаторів |

Отже, наукова новизна запропонованого методу полягає у створенні інноваційного механізму, що поєднує технології розподілених реєстрів, смарт-контрактів та криптографічного хешування для забезпечення достовірності, прозорості та безпеки державних реєстрів. На відміну від традиційних систем цей метод є стійким до загроз, мінімізує вплив людського фактора та забезпечує можливість реального аудиту операцій. Його впровадження дає змогу підвищити ефективність управління даними, забезпечити їх надійний захист та створити основу для цифрової трансформації державного сектору.

Використання блокчейн-технологій у державних реєстрах є не лише технічно доцільним, а й стратегічно важливим рішенням, що відповідає сучасним вимогам глобального інформаційного простору та підвищує рівень довіри до державних інституцій.

## Висновки

Розроблено інноваційний метод забезпечення достовірності та безпеки персональних даних у державних реєстрах на основі блокчейн-технологій. Запропонований підхід відповідає сучасним викликам у сфері захисту інформації, вирішуючи низку проблем, властивих традиційним централізованим системам управління даними.

По-перше, використання децентралізованої архітектури блокчейн забезпечує цілісність і незмінність даних у реєстрах. Це означає, що кожен запис у реєстрі захищений від несанкціонованих змін, а будь-які спроби маніпуляцій негайно стають очевидними завдяки механізму криптографічного хешування. Отже, система гарантує високий рівень захисту критично важливої інформації.

По-друге, впровадження смарт-контрактів дає змогу автоматизувати ключові процеси, такі як перевірка достовірності даних, контроль за доступом та виконання транзакцій. Це мінімізує людський фактор, який часто стає джерелом помилок або зловживань, і забезпечує ефективне управління даними. Крім того, автоматизація значно скорочує час на виконання операцій, що є особливо важливим для систем із високою інтенсивністю обробки даних.

По-третє, прозорість, яку забезпечує блокчейн, є ще однією важливою перевагою. Усі дії в системі реєструються і стають доступними для перевірки учасниками мережі. Такий підхід не тільки підвищує довіру громадян до державних інформаційних систем, а й забезпечує надійний аудит операцій, що виконуються в реєстрах.

Додатково, завдяки поєднанню блокчейну з іншими технологіями, такими як IPFS для зберігання великих обсягів даних, вдалося вирішити проблему масштабованості. Зберігаючи критичну інформацію безпосередньо в блокчейні, система розподіляє великий масив даних між вузлами, що забезпечує швидкий доступ і додатковий рівень надійності.

Практична реалізація запропонованого методу продемонструвала його ефективність у моделях блокчейн-реєстрів. Зокрема, результати показали підвищення стійкості системи до зовнішніх і внутрішніх загроз, значне покращення швидкості обробки транзакцій і зменшення ризику несанкціонованих змін даних. У реєстрах нерухомості, громадян або юридичних осіб впровадження цього методу дає змогу створити надійну систему, здатну підтримувати сучасні потреби державного управління.

Отже, запропонований метод є не лише технічним інструментом, а й стратегічним рішенням для підвищення ефективності державного управління. Він створює основу для більш прозорого, безпечного та ефективного надання послуг громадянам, що є ключовим фактором успіху в умовах цифрової трансформації.

## Список літератури

*1. Balatska V., Opirskyy I., 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. DOI: https://doi.org/10.18372/2225-5036.29.18073 (Accessed: 30 December 2024).*

*2. Балацька В., Побережник В., Опірський І. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619 (Accessed: 30 December 2024).*

*3. Poberezhnyk V., Balatska V., Opirskyy I. Development of the learning management system concept based on blockchain technology. CEUR Workshop Proceedings. 2023. Vol. 3550. URL: https://ceur-ws.org/Vol-3550/ (Accessed: 30 December 2024).*

*4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: https://bitcoin.org/bitcoin.pdf (Accessed: 30 December 2024).*

*5. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin Books, 2018.*

*6. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings of the 2017 IEEE International Congress on Big Data, 2017. Pp. 557–564. DOI: 10.1109/BigDataCongress.2017.85 (Accessed: 30 December 2024).*

*7. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. Blockchain Application Concept in SSO Technology Context. CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, 2024. Pp. 38–49. URL: https://ceur-ws.org/Vol-3654/ (Accessed: 30 December 2024).*

*8. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.*

*9. Балацька В., Побережник В., Опірський І. Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів. Кібербезпека: освіта, наука, техніка. 2024. № 4 (24). С. 99–114. DOI: https://doi.org/10.28925/2663-4023.2024.24.99114 (Accessed: 30 December 2024).*

*10. European Union Agency for Cybersecurity (ENISA) (2023). Blockchain Security: A Critical Analysis of Emerging Threats. URL: https://www.enisa.europa.eu (Accessed: 30 December 2024).*

*11. Balatska V., Slobodian N., Opirskyy I. Blockchain for enhancing transparency and trust in government registries. CPITS-II 2024, Kyiv, Ukraine, 2024. Pp. 50–59. URL: https://ceur-ws.org/Vol-3826/ (Accessed: 30 December 2024).*

*12. Nakamura K., Kobayashi H. Blockchain for Government Systems: Opportunities and Challenges. Journal of Cybersecurity and Digital Resilience. 2019. Vol. 10, Issue 2. Pp. 45–57.*

*13. Balatska V., Poberezhnyk V., Opirskyy I. Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. CEUR Workshop Proceedings. 2024. Vol. 3800. Pp. 70–80. URL: https://ceur-ws.org/Vol-3800/ (Accessed: 30 December 2024).*

*14. ISO/IEC 27001 (2022). Information security, cybersecurity and privacy protection — Information security management systems - Requirements. URL: https://www.iso.org/standard/82875.html (Accessed: 30 December 2024).*

*15. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. Blockchain Technology: Beyond Bitcoin. Applied Innovation Review. 2016. Issue 2. Pp. 6–19.*

*16. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30. Issue 2. Pp. 221–230. DOI: https://doi.org/10.18372/2225-5036.30.19211 (Accessed: 30 December 2024).*

*17. Deloitte Insights Blockchain for government: Real-world applications and challenges. 2021. URL: https://www2.deloitte.com/insights (Accessed: 30 December 2024).*

*18. Opirskyy I., Balatska V. Blockchain-based systems for public trust enhancement. International Journal of Digital Innovation. 2023. Vol. 12. Pp. 102–118.*

*19. European Commission. Blockchain for Digital Government: Future Perspectives and Policies. 2022. URL: https://ec.europa.eu/digital-blockchain (Accessed: 30 December 2024).*

*20. Kshetri N., Voas J. Blockchain in Developing Countries. IT Professional. 2018. Vol. 20. Issue 2. Pp. 11–14. DOI: https://doi.org/10.1109/MITP.2018.021921645 (Accessed: 30 December 2024).*

# DEVELOPMENT OF A METHOD FOR ENSURING THE RELIABILITY AND SECURITY OF PERSONAL DATA IN BLOCKCHAIN SYSTEMS OF STATE REGISTERS

**V.S. Balatska [1,2], V.O. Poberezhnyk [2], A.V. Stefankiv [2], Yu.A. Shevchuk [2,3]**

[1] Lviv State University of Life Safety,
Department of Information Security Management
[2] Lviv Polytechnic National University,
Department of Information Protection
[3]DataArt, Northbrook, Illinois, USA.
*E-mail: v.balatska@ldubgd.edu.ua, valeriia.s.balatska@lpnu.ua, , vasyl.poberezhnyk@gmail.com, artem.stefankiv.mkbas.2024@lpnu.ua, shev4ukyuri@gmail.com*



**The article considers the problem of ensuring the reliability and security of personal data processed in state registers by using blockchain technologies. The growing requirements for transparency and stability of state data management systems pose new challenges to protecting information from unauthorized changes, interference, and forgery. A method based on implementing a decentralized blockchain architecture is proposed to ensure data integrity, traceability, and transparency during processing and storage.**

**The basis of the developed method is the use of a distributed registry, which ensures the immutability of the entered information thanks to the mechanism of blockchains that link transactions and changes in data in chronological order. Smart contracts are used to automate the processes of entering, updating, and verifying data in state registers, which reduces the likelihood of the human factor and ensures trust between all participants in the system.**

**The proposed method increases state registers' resistance to external threats, internal errors, and unauthorized changes due to the transparency and decentralization inherent in blockchain technologies. The practical implementation of the method demonstrated an improvement in the level of security of personal data and the efficiency of the functioning of registration systems using the example of modeling a blockchain register.**

**Keywords: blockchain, data reliability, state registers, decentralization, information security, smart contracts, distributed register.**