КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.99114
УДК 004.056.5

Балацька Валерія Сергіївна
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-6262-6792
valeriia.s.balatska@lpnu.ua

Побережник Василь Олегович
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-7523-2557
vasyl.poberezhnyk@gmail.com

Опірський Іван Романович
д.т.н., професор, професор кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ВИКОРИСТАННЯ NON-FUNGIBLE TOKENS ТА БЛОКЧЕЙН ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДЕРЖАВНИХ РЕЄСТРІВ

Анотація. В сучасному світі, де цифрові технології відіграють все більш важливу роль у різних аспектах життя, захист даних та забезпечення їх конфіденційності та цілісності стає все більш актуальним завданням. Особливо важливою є ця проблема в контексті державних реєстрів, які містять великий обсяг цінної інформації про громадян, бізнес та інші суб'єкти. Розмежування доступу до державних реєстрів є ключовим завданням для забезпечення безпеки, прозорості та ефективності управління даними в урядових органах. У цьому контексті використання Non-Fungible Tokens (NFT) та технології блокчейну може стати перспективним рішенням. Ця стаття розглядає можливості використання NFT та блокчейну для розмежування доступу до державних реєстрів в Україні. У даній роботі визначаються ключові поняття, такі як NFT, блокчейн, ідентифікація, автентифікація та управління доступом і розглядаються їхні можливі застосування для розмежування доступу до державних реєстрів. Також описується, як використання технологій блокчейну та NFT може стати ключовим рішенням для забезпечення безпеки та ефективності управління державними реєстрами. Блокчейн, як розподілена база даних, забезпечує надійне зберігання історії транзакцій та непереборне шифрування даних. Кожен блок у ланцюжку має унікальний хеш, який зв'язує його з попереднім блоком, що робить будь-яку спробу змінити дані в блоках майже неможливою без виявлення. З іншого боку, NFT можуть служити унікальними цифровими ідентифікаторами, які визначають права доступу до конкретних даних в державних реєстрах. Кожен NFT містить унікальний цифровий підпис, що підтверджує його власність та характеристики, і може бути використаний для точного визначення прав доступу до конкретних даних чи ресурсів. Разом ці технології можуть створити надійну та безпечну інфраструктуру для управління державними реєстрами, забезпечуючи прозорість, конфіденційність та невідворотність транзакцій.

Ключові слова: блокчейн; Non-Fungible Tokens (NFT); авторизація; ідентифікація; розмежування доступу; децентралізація.

ВСТУП

Блокчейн — це розподілений децентралізований реєстр, іноді його також називають базою даних, який зберігає транзакції у хронологічному порядку у незмінному вигляді та пов'язує їх між собою. Сьогодні багато угод (транзакцій) відбуваються не безпосередньо

між окремими учасниками, а за посередництвом контролюючого органу, так званого посередника. Наприклад, банк перевіряє, чи достатньо грошей у відправника переказу і чи є одержувач, і гарантує, що гроші надійдуть до одержувача і одночасно будуть списані з відправника. Такі посередники зустрічаються не тільки у фінансової сфері, а й у державному секторі, де відбувається передача цінностей (наприклад, грошей, прав власності).

Використання блокчейн та NFT для розмежування доступу до державних реєстрів в Україні може забезпечити високий рівень безпеки та прозорості. Блокчейн може служити основою для зберігання даних, забезпечуючи їх недоступність для несанкціонованого доступу. NFT можуть використовуватися для унікальної ідентифікації користувачів та надання прав на конкретні частини інформації. Це може покращити відстеження доступу та управління правами в державних реєстрах.

Впровадження блокчейну та NFT у державні реєстри України має потенціал зробити систему більш ефективною та надійною. Блокчейн, як розподілена система зберігання даних, дозволяє створити непередбачуваний рівень безпеки. Кожен блок інформації зв'язаний з попереднім та зашифрований, забезпечуючи відмінність та неприпустимість змін.

NFT, або не передавальні токени, можуть бути використані для унікальної ідентифікації користувачів та надання прав доступу. Кожен користувач може мати свій унікальний токен, що визначає обсяг інформації, до якої він має доступ. Це сприяє забезпеченню конфіденційності та контролю за рівнем доступу.

Постановка проблеми. Полягає у тому, що існуючі системи управління державними реєстрами в Україні можуть бути недостатньо ефективними, недостатньо прозорими та вразливими до корупції та фальсифікації даних. Традиційні централізовані системи можуть страждати від проблем, таких як обмежений доступ до інформації, недовіра до цілісності даних, а також складність у впровадженні механізмів захисту від кібератак. До того ж, існуючі процедури аутентифікації та авторизації є недостатньо надійними, що призводить до ризику зловживання доступом до реєстрів.

Нерідко інформація може бути підвернена змінам або видаленням без сліду. Ці проблеми можуть призвести до порушень прав громадян, втрати довіри до державних інституцій та економічних втрат. Одним зі способів вирішення цих проблем є використання технологій блокчейн та NFT. Ці технології можуть забезпечити прозорість та відстежуваність даних, знижуючи ризик фальсифікації та забезпечуючи вищий рівень довіри до інформації у державних реєстрах. Однак, виникають нові виклики, такі як потреба у вирішенні технічних, організаційних та правових аспектів, щоб успішно впровадити ці технології в державному секторі.

Також необхідно враховувати можливість опору чи недовіри громадськості до нововведень, що може вплинути на прийняття та успішність проєкту.

Аналіз останніх досліджень і публікацій. У сучасному світі цифрові технології стають все більш важливими для ефективного управління державними реєстрами та забезпечення їх безпеки та прозорості. Одним із потенційних рішень для цього є використання технологій блокчейну та NFT, які можуть забезпечити ненадійність даних та ідентифікації, а також ефективне управління доступом до реєстрів. Дослідження можливостей та переваг використання таких технологій для розмежування доступу до державних реєстрів [1] є одним із важливих завдань сьогодення.

Технології блокчейну та NFT можуть допомогти вирішити проблеми, пов'язані з управлінням доступом до державних реєстрів. Тому важливо проаналізувати можливі ризики та перешкоди, які можуть виникнути при впровадженні цих технологій в контексті українського законодавства та інфраструктури. Розгляд технічних аспектів

використання блокчейну та NFT для управління доступом до державних реєстрів є вирішальним аспектом для дослідження цієї теми для українського простору і не тільки.

Останні дослідження в галузі блокчейну та NFT відображають постійний інтерес до цих технологій та їхнього потенціалу у різних сферах, включаючи управління державними реєстрами. Дослідники вивчають можливості використання блокчейну та NFT для безпечного та ефективного управління даними урядових реєстрів. Це включає реєстрацію власності, ідентифікацію громадян, адміністративні послуги та інші аспекти управління даними. Також, дослідження фокусуються на тому, як блокчейн може забезпечити прозорість та надійність даних у державних реєстрах. Вони вивчають можливості створення незмінних, ідентифікованих та доступних для перевірки записів.

Безпека та приватність є ключовими аспектами дослідження, вчені шукають способи захисту конфіденційності даних у реєстрах за допомогою технологій блокчейн, зокрема шифрування та розробки приватних блокчейнів. Дослідження охоплюють аналіз юридичних і регуляторних викликів у використанні блокчейн та NFT у державних реєстрах. Це включає вивчення нормативного середовища, визначення правових аспектів власності та конфіденційності. Деякі дослідження досліджують конкретні випадки впровадження систем на основі блокчейну та NFT у державних реєстрах. Вони аналізують переваги, виклики та можливості таких рішень у реальних умовах [2].

Загалом, останні дослідження та публікації підтверджують широкий спектр можливостей та викликів у використанні блокчейну та NFT для управління державними реєстрами, а також створюють базу знань для подальшого розвитку цих технологій у цій сфері.

Мета статті. Метою статті є дослідження можливостей та переваг використання технологій блокчейн та NFT для розмежування доступу до державних реєстрів в Україні, а також у виявленні та аналізі проблем, які можуть виникнути при впровадженні таких технологій.

Основними завданнями статті є:

1. Дослідження можливостей використання технології блокчейн для контролю доступу до даних. Це включає аналіз можливостей створення розподіленої системи контролю доступу на основі блокчейн та визначення оптимальних підходів до реалізації такої системи.
2. Вивчення принципів роботи NFT та їхнього використання для ефективного розмежування доступу до даних. Це може включати аналіз методів створення та використання NFT для ідентифікації користувачів та надання їм відповідних прав доступу.
3. Аналіз можливостей використання криптографії у блокчейні для забезпечення безпеки та конфіденційності даних. Це може включати дослідження різних криптографічних методів, таких як шифрування та цифровий підпис, і їхнє застосування для захисту даних у системі блокчейн.
4. Розробка концепції системи з використанням технології блокчейн, NFT та IPFS для забезпечення безпечного обміну даними. Це включає визначення архітектури системи, вибір необхідних компонентів та розробку стратегії впровадження та масштабування системи.
5. Технічна реалізація розробленої концепції та випробування її працездатності. Це може включати розробку програмного забезпечення для створення та управління NFT, налаштування блокчейн мережі для зберігання даних та інтеграцію з IPFS для ефективного зберігання великих обсягів даних.

6. Оцінка ефективності та безпеки розробленої системи. Це може включати проведення тестів на надійність та безпеку, аналіз результатів та внесення необхідних коригувань для підвищення якості системи.

Ці завдання допоможуть створити ефективну та безпечну систему для обміну даними з використанням технологій блокчейн, NFT та IPFS.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Блокчейн та NTF для ефективного розмежування доступу

Блокчейн та NFT (Non-Fungible Tokens) — це дві різні, але пов'язані технології, які здатні революціонізувати способи управління даними та цифровими активами [3].

Блокчейн — це розподілена база даних, яка зберігається на різних комп'ютерах одночасно, що утворюють мережу. Кожен блокчейн записується у блоках, які зв'язані криптографічно та утворюють ланцюжок. Ця технологія стала відомою завдяки криптовалюті, зокрема Bitcoin, але її потенціал виявився набагато ширшим. Вона може використовуватися для безпечного та надійного зберігання різних видів інформації, від фінансових транзакцій до медичних записів та голосування.

NFT (Non-Fungible Tokens) — це цифрові активи, які відмінні від традиційних криптовалют, таких як Bitcoin чи Ethereum, тому що вони є унікальними та незамінними. Кожен NFT містить унікальний цифровий підпис, який підтверджує його власність та характеристики. NFT використовуються для представлення цифрових медіаоб'єктів, таких як мистецькі твори, музика, відео, гіфки тощо, і надають їм вартість та унікальність.

Разом ці технології можуть використовуватися для створення нових моделей власності, де цифрові активи можуть бути унікальними, незамінними та перевіреними за допомогою блокчейну [4]. Наприклад, за допомогою NFT можна відслідковувати власність цифрових мистецьких творів, а блокчейн може забезпечити надійність та прозорість транзакцій. Переваги включають високий рівень прозорості, відсутність посередників та можливість відслідковування всіх змін у системі. Однак важливо враховувати виклики, такі як технічна складність впровадження, правові аспекти та забезпечення відмовостійкості системи.

Впровадження технологій блокчейн та NFT у державні реєстри може сприяти боротьбі з корупцією та підвищити довіру громадськості. Блокчейн забезпечить невідворотний слід у кожній транзакції чи записі, знижуючи можливість фальсифікації.

Надійне визначення прав доступу за допомогою NFT дозволить точно контролювати, хто, коли і яку інформацію може переглядати чи змінювати [5]. Це може підвищити конфіденційність особистих даних та іншої чутливої інформації.

Однак успіх такого проекту вимагатиме широкого впровадження та співпраці між різними галузями уряду, технологічними компаніями та експертами з безпеки. Важливо також врахувати питання конфіденційності, ефективності та легальності використання таких технологій в сфері державних реєстрів.

Також варто враховувати важливі аспекти для впровадження даної системи, зокрема:

– Стандартизація. Розробка і прийняття стандартів є важливою для того, щоб різні системи, що використовують блокчейн та NFT, могли взаємодіяти між собою. Стандарти дозволять забезпечити сумісність та обмін даними між різними блокчейн-платформами, що є критичним для ефективної роботи системи реєстрів.

- Економічний вплив. Дослідження економічного впливу впровадження блокчейну та NFT допоможе оцінити ефективність та вигоди для державних служб. Аналіз витрат та користей допоможе визначити, чи це ефективне інвестування для держави.
- Освіта та прийняття. Розробка освітніх програм є ключовою для підготовки персоналу та громадськості до використання нових технологій. Це може включати навчання з аспектів технічної реалізації, а також засвоєння засад конфіденційності та безпеки даних.
- Співпраця із сектором приватного бізнесу. Партнерство з технологічними компаніями може забезпечити доступ до експертів та ресурсів для успішної реалізації проекту. Співпраця може сприяти розвитку інновацій та прискорити впровадження нових технологій.
- Залучення зацікавлених сторін. Врахування потреб та думок різних груп, таких як громадяни, правозахисні організації та інші, допоможе забезпечити широку підтримку для проекту. Важливо вести відкритий діалог та враховувати різні точки зору.
- Міжнародний досвід. Вивчення досвіду інших країн у використанні блокчейну та NFT у державних реєстрах дозволяє уникати можливих помилок та використовувати найкращі практики. Міжнародна співпраця може також сприяти обміну знаннями та технологіями.

Таблиця 1

Переваги та недоліки впровадження блокчейну та NFT в державні реєстри

Переваги	Недоліки
1. Забезпечення високого рівня захисту від несанкціонованого доступу та фальсифікації даних. 2. Створення прозорої системи, де всі транзакції та зміни в реєстрах є відкритими та доступними для перевірки. 3. Використання NFT для точного визначення прав доступу, що сприяє ефективному контролю та обмеженню доступу до конкретної інформації. 4. Зменшення можливості корупції та підвищення довіри громадськості до державних реєстрів.	1. Розробка та впровадження таких систем може бути складною через потрібність великого обсягу технічних ресурсів. 2. Необхідність вирішення юридичних аспектів, таких як захист особистих даних, визнання легальності NFT, та забезпечення відповідності законодавству. 3. Важливо враховувати можливість відмови та забезпечення стійкості системи до атак та технічних проблем. 4. Велика витрата часу, грошей і людських ресурсів на впровадження та підтримку таких технологій.

Блокчейн для контролю доступу

Застосування технології блокчейн для контролю доступу є однією із значущих областей в сучасному світі інформаційної безпеки. Блокчейн може служити основою для створення надійних та безпечних систем управління доступом до різних ресурсів, будь то фізичні об’єкти, цифрові активи або конфіденційна інформація [6].

Варто виділити ключові аспекти використання блокчейн для контролю доступу:

1. Одним з головних переваг блокчейн є його децентралізована природа. Замість централізованих систем управління доступом, які можуть стати мішенню для кібератак або зловмисних дій, блокчейн дозволяє розподілену систему, де дані зберігаються на різних вузлах мережі.

2. Інформація про права доступу та ідентифікаційні дані можуть бути записані у блокчейн як надійні дані. Це означає, що вони не можуть бути змінені або видалені без консенсусу мережі, що робить систему більш надійною та стійкою до зловживання.
3. Блокчейн може підтримувати смарт-контракти — програмні коди, які автоматизують та контролюють виконання умов угод. Це дозволяє створювати автоматизовані системи управління доступом, які діють безпосередньо на основі певних умов.
4. Блокчейн може бути використаний для зберігання криптографічних ключів та ідентифікаційних даних, що дозволяє забезпечити безпеку доступу до систем та ресурсів.
5. Блокчейн забезпечує трасуваність операцій, що дозволяє проводити детальний аудит доступу та використання ресурсів. Це допомагає виявляти та запобігати недозволеному доступу чи зловживанню.

Отже, використання блокчейн для контролю доступу може покращити безпеку, прозорість та ефективність управління доступом до різноманітних ресурсів, що є критично важливим для захисту конфіденційної інформації та запобігання кіберзлочинності.

Також варто згадати і про звичайні методи підпису, такі як хмарний ключ, біометричний ключ та файловий ключ ЕЦП, що використовуються для забезпечення безпеки та контролю доступу до різних ресурсів. У порівнянні з цими методами, метод, що базується на технології блокчейну, NFT та IPFS, може забезпечити вищий рівень безпеки, прозорості та ефективності управління доступом, розглянемо це детальніше у табл. 2.

Таблиця 2

Порівняльний аналіз методів підпису та методу з використанням блокчейну, NFT та IPFS

Характеристика	Хмарний ключ	Біометричний ключ	Файловий ключ ЕЦП	Блокчейн, NFT та IPFS
Зручність	Потребує доступу до Інтернету та довіри до хмари.	Вимагає наявності біометричних даних користувача.	Потребує зберігання файлу з ключем.	Може потребувати підключення до мережі, потребує наявного криптогаманця (пари: відкритий–закритий ключ).
Безпека	Потенційно вразливий до кібератак.	Можливість підробки або обману біометричних даних.	Вимагає захищеності файлу ключа.	Ключ практично неможливо підібрати, вразливий до викрадення чи втрати ключа.
Простота використання	Легко доступний, але вимагає авторизації.	Залежить від доступності біометричних сенсорів.	Потребує доступу до файлу та програмного забезпечення.	Потребує використання технології блокчейн, яка не є загальновживаною.
Відновлення	Залежить від можливостей хмарного сервісу.	Не можливе відновлення при втраті біометричних даних.	Потребує створення резервних копій ключа.	Відновлення втраченого ключа практично неможливе.
Вартість	Залежить від хмарного провайдера.	Може вимагати витрат на біометричне обладнання.	Вартість зберігання та захисту файлу ключа.	Вартість залежить від розробки та впровадження технології блокчейну та NFT.

З таблиці видно, що метод, який базується на використанні блокчейну, NFT та IPFS, має декілька переваг порівняно з іншими методами підпису, а саме:

1. Запропонований метод забезпечує високий рівень безпеки за рахунок застосування технології блокчейну, яка гарантує надійність і недоступність для зловмисників.
2. Використання блокчейну дозволяє забезпечити прозорість операцій та недоступність для маніпуляцій.
3. Завдяки механізмам блокчейну та NFT, можливе відновлення доступу до даних у разі втрати ключа чи інших непередбачених ситуацій.
4. Метод забезпечує простоту використання для користувачів без необхідності у спеціальних біометричних даних або складних файлових ключах.

Отже, на основі порівняльного аналізу можна зробити висновок, що використання методу з використанням блокчейну, NFT та IPFS є ефективним та переважним з точки зору безпеки, прозорості та зручності використання.

Криптографія у блокчейн

Приватні ключі. Роль приватного ключа відіграє випадкове значення. Керування даним ключем є основою управління крипто гаманцем та пов'язаним із ними активами. Він використовується для підписування транзакції, які будуть створені власником крипто гаманця та підтвердити автентичність даних транзакцій. Також, даний ключ дозволяє отримувати доступ не тільки до криптовалюти, яка знаходиться у крипто гаманці, але й до смарт-контрактів, NFT та будь-яких інших активів, які можуть бути пов'язані із крипто гаманцем [7].

Варто пам'ятати, що даний ключ являється єдиним методом для отримання доступу до крипто гаманця, відповідно його втрата чи несанкціонований доступ до нього може призвести до втрати доступу до гаманця та пов'язаних з ним активами. Оскільки відновлення приватного ключа в мережі блокчейн є неможливим.

Зважаючи на важливість приватного ключа, стає зрозумілим те, що його генерація має відбувати випадково, що забезпечить неможливість підбору параметрів генератора для зловмисного відтворення приватного ключа. Існує кілька підходів, які дозволять забезпечити випадковість згенерованого ключа.

Публічні ключі. Генерація публічного ключа відбувається за допомогою застосування еліптичних кривих. Ці криві грають важливу роль у криптографії, зокрема в криптовалютних системах, таких як Bitcoin та Ethereum. Їхнє застосування дає можливість генерації ключів шифрування та підпису, що, у свою чергу, використовуються для створення адрес гаманців та здійснення транзакцій. Еліптичні криві дозволяють генерувати ключі шифрування, які складаються з двох частин: приватного ключа та відповідного йому публічного ключа. Приватний ключ є секретним числом, а публічний ключ — це точка на еліптичній кривій, що обчислюється за допомогою приватного ключа та початкової точки генератора.

$$K_{pub} = K_{pr} \times P_g \ (1),$$

де K_{pub} — публічний ключ, K_{pr} — приватний ключ, P_g — початкова точка генератора. Результуючий публічний ключ є результатом «множення» на еліптичних кривих. Відмінність даної операції множення полягає в тому, що для неї не існує інверсної операції, тобто операції ділення, і варіантом для пошуку приватного ключа є розв'язання проблеми дискретного логарифму, що перетворює спробу знаходження приватного ключа у нетривіальну задачу, що потребує значних обчислювальних потужностей. Зважаючи на довжину приватного ключа, яка становить 256 біт, розв'язання такої задачі вважається

неможливим [8]. Отже, застосування еліптичних кривих дозволяє забезпечити високу стійкість до атак та безпеку при використанні коротких ключів, що робить їх ідеальними для застосування у таких системах як Bitcoin, Ethereum.

Адрес гаманця у криптовалютних системах, визначається на основі публічного ключа. Зазвичай він отримується за допомогою хеш-функцій та інших алгоритмів, які перетворюють публічний ключ у вигляд, зрозумілий для користувачів, і стає адресою, на яку можна надсилати, наприклад, криптовалюту. Підпис транзакцій використовується для підтвердження автентичності та цілісності транзакції у криптовалютних системах. Зважаючи на це, криптографічна пара з публічного та приватного ключа, може відігравати роль ідентифікатора користувача.

Варіанти застосування

Для розмежування доступу до державних реєстрів в Україні може бути дієвим і ефективним рішенням. Це може працювати як, кожен користувач блокчейн може мати свої унікальні ключі: приватний ключ, який залишається конфіденційним і використовується для підпису транзакцій, і публічний ключ, який відомий всім і використовується для перевірки цифрового підпису. Кожна транзакція у блокчейн підписується за допомогою приватного ключа користувача. Публічний ключ використовується для перевірки автентичності підпису. Це забезпечує, що тільки власник приватного ключа може здійснювати транзакції від його імені.

Наступним кроком є те, що кожен користувач може бути ідентифікований за допомогою його публічного ключа, який є унікальним ідентифікатором у мережі [9]. Це дозволяє розрізняти та відстежувати дії кожного учасника у системі. За допомогою криптографічних методів можна регулювати доступ до різних частин державних реєстрів. Наприклад, можна створити «розумні контракти», які перевіряють цифрові підписи користувачів перед наданням їм доступу до конкретних даних чи функцій реєстру.

Криптографія забезпечує високий рівень безпеки, оскільки ключі є важко зламати. Крім того, блокчейн забезпечує надійність даних, що робить систему стійкою до втручання чи видалення даних. Використання криптографії як ідентифікатора у блокчейн дозволяє створити надійну та безпечну систему для розмежування доступу до державних реєстрів в Україні.

Залежно від конкретних потреб та вимог, застосування криптографії у блокчейн для розмежування доступу до державних реєстрів в Україні може включати різні аспекти та методи.

1. Ідентифікація та аутентифікація. Криптографічні методи можуть використовуватися для ідентифікації учасників мережі та перевірки їх автентичності. Кожен користувач може мати унікальний цифровий ідентифікатор, що базується на його публічному ключі, який відомий у мережі.
2. Цифровий підпис. Кожна транзакція чи запит на доступ до реєстру може бути підписана за допомогою приватного ключа користувача. Це забезпечує цілісність та автентичність операцій, оскільки можна перевірити, що вони були створені відповідним користувачем.
3. Розумні контракти. У блокчейн можна реалізувати розумні контракти, які автоматично виконуються при виконанні певних умов. За допомогою криптографії можна створити розумні контракти, які регулюють доступ до даних реєстру на основі цифрових підписів та ідентифікаторів користувачів.

5. Шифрування даних. Криптографічні методи можуть бути використані для шифрування конфіденційної інформації у державних реєстрах. Це дозволить захистити дані від несанкціонованого доступу та забезпечить конфіденційність особистої інформації громадян.
6. Мультипідписи. Криптографічні методи також можуть бути використані для створення мультипідписів, де доступ до державних реєстрів може бути контрольований групою учасників, кожен з яких має свій власний приватний ключ.

Ці підходи дозволяють створити надійну та безпечну систему для розмежування доступу до державних реєстрів в Україні, яка забезпечує цілісність, автентичність та конфіденційність даних. Однак важливо ретельно розробити та реалізувати криптографічні заходи з урахуванням всіх вимог безпеки та приватності.

Концепція системи

Концепція пропонованої системи полягає у забезпеченні безпечного обміну даними через застосування можливостей технології блокчейн, NFT та IPFS [10]. Зважаючи на можливості та властивості згаданих технологій, такий підхід дозволить забезпечити обмін даними при збереженні таких ключових властивостей інформації як достовірність, цілісність та доступність.

Застосування IPFS зумовлено тим, що обмін відносно великими даними в блокчейні є недоцільним та не вигідним [11], а згадана технологія дозволяє зберігати відносно великі дані в порівнянні із розміром блоку без впливу на саму мережу блокчейн.

Керування доступом до даних в даному підході забезпечується використанням NFT, оскільки дані токени дозволяють зберігати необхідну інформацію для забезпечення розмежування доступу, а їхнє функціонування в мережі блокчейн дозволяє забезпечити захист даних про дозволи через саму природу блокчейну. На рис. 1 наведено схематичне зображення NFT, який застосовується для надання доступу до даних.

Отже, інформація в запропонованому NFT буде містити необхідні дані для забезпечення процесу обміну інформацією між сторонами. Важливими полями в даній структурі є ті, що відповідають за ідентифікацію творця даних, адресата та геш-даних. Ідентифікатор творця дозволить переконатися в тому, що дані були створені довіреною стороною, ідентифікатор адресата дозволить переконатися в тому, що доступ намагається отримати саме авторизований для цього користувач, а геш-даних відіграватиме одночасно дві ролі:

1. Геш-даних дозволить переконатися в цілісності даних, оскільки його невідповідність буде свідчити про внесені зміни.
2. Геш-даних використовується для пошуку даних в IPFS [12].

Зважаючи на це застосування NFT, як способу керуванням доступом дає можливість не тільки розмежувати доступ до даних, якими обмінюються, але й забезпечити контроль цілісності да достовірність інформації.

Складовими даної системи буде блокчейн мережа, яка одночасно відіграє роль бази даних користувачів системи та NFT-доступу і IPFS-мережа, яка відповідає за збереження самих даних та контроль доступу до них.

Дана система працюватиме за таким алгоритмом:

1. Користувач А хоче надіслати дані користувачу Б.
2. Користувач А завантажує у IPFS, отримує геш-даних та створює NFT в якому вказує користувача Б, як авторизованого користувача та геш-даних.
3. NFT додається в блокчейн.

ISSN 2663 - 4023

4. Користувач Б надсилає запит на отримання даних у IPFS систему та надає дані для перевірки.
5. IPFS перевіряє ідентифікатор користувача Б. Якщо користувач проходить перевірку, система надає йому доступ до даних, якщо ні — запит відхиляється.

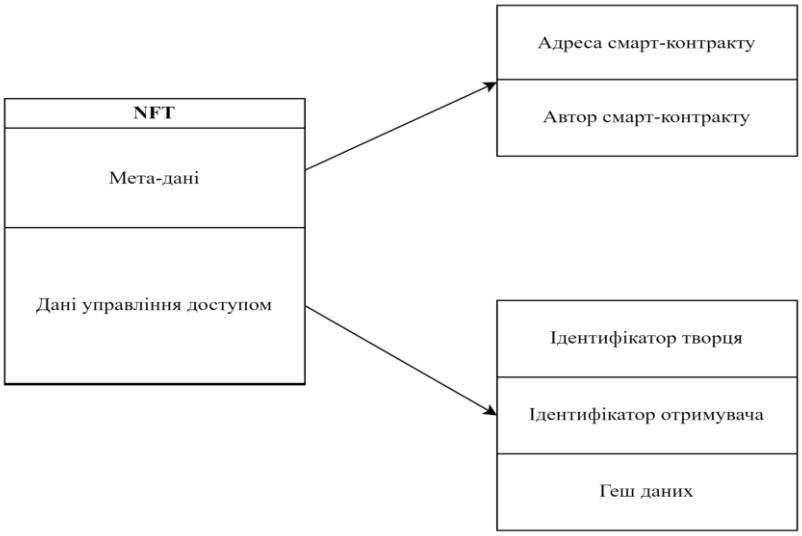

Рис.1. Структура токену доступу

Концептуальна схема даної системи зображено на рис. 2.

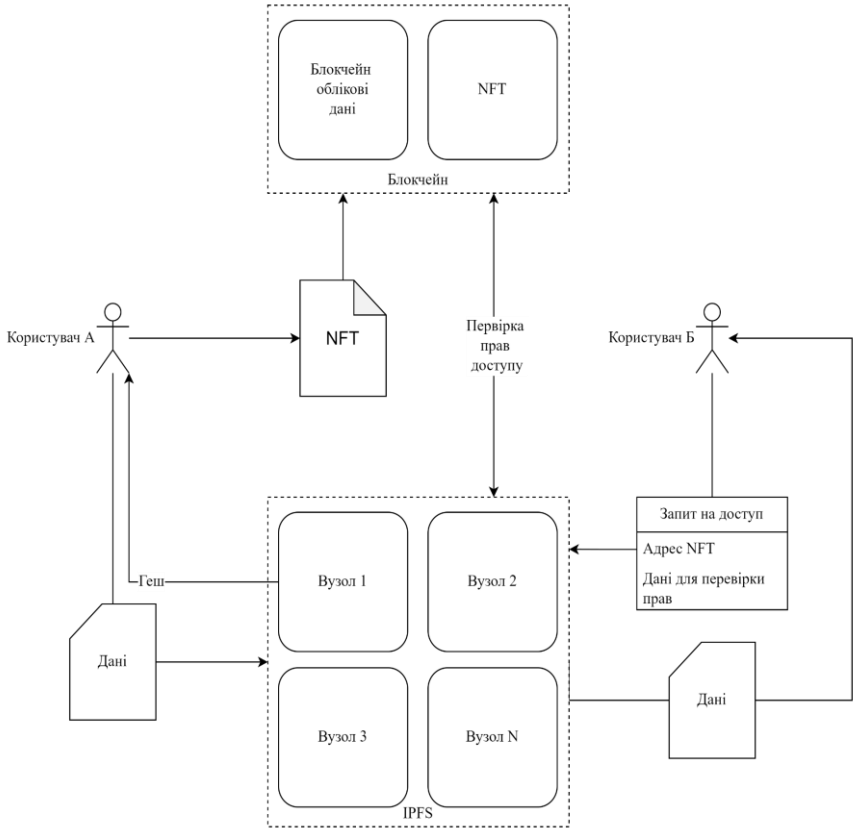

Рис. 2. Концептуальна схема системи

Недоліки та переваги даної концепції розглянуто в табл. 3.

Дана система надає ряд переваг, зокрема децентралізоване сховище, збереження таких характеристики інформації як цілісність та доступність, через застосування децентралізованих технології для надання доступу та збереження інформації в мережі. А також забезпечення стійкості до несанкціонованих змін через перевірку хешів збережених даних, оскільки такий хеш одночасно використовується для пошуку даних в IPFS і зберігається, як контрольна сума в самому смарт-контракті, що дозволить мінімізувати ризик надання користувачу інформації, що містить несанкціоновані зміни, оскільки невідповідність хешу самих даних та збереженого в смарт-контракті буде свідчити про втручання, а також сама IPFS не зможе надати користувачу не змінені дані, оскільки їхній геш не буде збігатися із гешом, який використовується для пошуку.

Дані можливості пропонованої системи дозволяють розглядати її як можливу для застосування, втім згадані недоліки, потребують розгляду та пошуку можливих способів їхнього вирішення чи мінімізації.

Таблиця 3

Переваги, недоліки та проблеми запропонованої концепції

Переваги	Недоліки	Проблеми
1. Забезпечення цілісності інформації. 2. Забезпечення доступності інформації. 3. Збільшення стійкості системи до атак спрямованих на відмову в обслуговуванні через застосування децентралізації. 4. Прозорість мережі. 5. Оптимізації використання простору в блокчейну, через збереження файлів у IPFS.	1. Транзакції в мережі доступні всім користувачам. 2. Зниження рівня децентралізації мережі через застосування двох різних типів підсистем (IPFS та Блокчейн). 3. Розробка додаткового функціоналу смарт-контрактів збільшуватиме вартість функціонування мережі. 4. Потенційне зниження швидкодії мережі блокчейн через збільшення розміру мережі із ростом кількості транзакцій. 5. Втрата приватного ключа призводить до втрати контролю над даними в IPFS.	1. Складність інтеграції різних технологій та підсистем. 2. Вибір найбільш оптимального архітектурного рішення. 3. Виявлення та усунення можливих вразливостей та атак системи. 4. Розробка механізмів резервного копіювання та відновлення ключів. 5. Оптимізація та підтримка високої продуктивності. 6. Розробка механізмів автоматичного масштабування системи.

Зокрема, одна з переваг застосування мережі блокчейн та NFT — це прозорість мережі та відкритість, що дає можливість будь-якому користувачу перевірити мережу, впевнитися в її безпечності чи взяти участь у підтримці функціонуванні мережі. Однак, дана властивість, також дає можливість зловмисникам аналізувати мережу, шукати користувачів, які часто обмінюються даними, доєднуватися до мережі в ролі зловмисних вузлів тощо. Очевидно, що дана характеристика є дуальною за своєю природою і одним з можливих способів вирішення даної проблеми є застосування інших типів блокчейну, зокрема приватного, гібридного чи інших. Такий підхід дозволить керувати інформацією, яку можуть бачити користувачі блокчейну, регламентувати доєднання нових вузлів в мережу тощо. Однак, основним недоліком такого вирішення проблеми буде падіння рівня децентралізації, оскільки застосування таких типів блокчейну призведе до появи в мережі привілейованих вузлів.

Ще одним недоліком є зниження децентралізації через розподіл системи на дві підсистеми — сам блокчейн та IPFS. Даний недолік неможливо обійти, саме наявність IPFS в загальній системі дозволяє знизити навантаження на блокчейн, через винесення даних, якими обмінюються, за межі блокчейну. Дана необхідність обумовлена тим, що саме збереження умовно великих даний є недоцільним, оскільки це негативно впливатиме на розмір блокчейну та його швидкодію. Також наявність таких даних у відкритому блокчейні може призвести до отримання несанкціонованого доступу до них, оскільки такий блокчейн не дає можливості керування доступом до даних, а завжди обробляє їх у відкритому виді.

Також, вагомою перепоною в розробці такої системи може стати складність смарт-контрактів. Складність вирішення даної проблеми полягає у вартості самих смарт-контрактів, оскільки вартість завантаження розумного контакту у мережу блокчейн напряму залежить від його розміру, а розмір контракту залежить від його складності. Вирішенням даної проблеми може стати розробка смарт-контрактів, які будуть покривати мінімально необхідний функціонал, який забезпечуватиме контроль доступу. А додатковий функціонал, наприклад оповіщення про наявність нових даних для користувача, оповіщення про доступ до даних тощо, винести за межі технології блокчейн та організувати їх за допомогою технологій більш пристосованих для швидкого обміну інформацією. Однак, варто зважати на те, що застосування додаткових технологій несе в собі нові ризики, які будуть пов’язані із конкретними технологіями.

Також, важливим недоліком, яким не можна нехтувати є можлива втрата приватного ключа. Даний ключ, як згадувалося раніше, гарантує повний доступ до криптогаманця користувача та активів пов’язаних з ним. А в самій технології блокчейн не існує механізму для відновлення доступу до втраченого ключа. Частково, дану проблему вирішує мнемонічна фраза [13], втім наявність такої фрази теж несе в собі дуальність. Вона одночасно дозволяє відновити доступ до втраченого гаманця, але також її компрометація дозволить зловмиснику отримати повний доступ до криптогаманця та, відповідно, приватного ключа. Відповідно, компрометація такої фрази несе в собі загрозу отримання несанкціонованого доступу до всієї інформації, якою обмінювалися впродовж існування криптогаманця. Оскільки компрометація може бути непоміченою, це може призвести існування витоку інформації впродовж тривалого часу [14], поки даний витік не буде помічено. Відповідно, дана проблема потребуватиме пошуку вирішення. Зокрема одним з можливих варіантів захисту, є тимчасове зберігання даних в IPFS, що дозволить обмежити кількість інформації, яка може бути викрадена при отриманні зловмисником доступу до приватних ключів, які використовувалися впродовж тривалого часу. Також додатковим методом захисту може стати введення додаткового криптографічного захисту. Однак, дане рішення потребуватиме розробки методу обміну ключами дешифрування, що призводитиме до додаткового ускладнення системи.

ВИСНОВКИ

У цій роботі розглянуто технології блокчейну та Non-Fungible Tokens (NFT) і їх потенціал для революціонізації управління даними та цифровими активами. Блокчейн забезпечує розподілену базу даних з криптографічно зв’язаними блоками, що надає безпечне зберігання різноманітної інформації. NFT визначають унікальні цифрові активи, які надають вартість та унікальність цифровим об’єктам.

Впровадження цих технологій у державні реєстри може мати великий потенціал для боротьби з корупцією, забезпечення відкритості та прозорості, а також підвищення довіри громадськості. Проте, перед впровадженням необхідно вирішити ряд технічних, юридичних та організаційних питань, включаючи стандартизацію, економічний вплив, освіту та прийняття, співпрацю з приватним сектором та залучення зацікавлених сторін.

Успішна реалізація даного проєкту може вимагати широкої співпраці та партнерства між різними галузями, а також врахування міжнародного досвіду та кращих практик. Важливо також забезпечити високий рівень конфіденційності, ефективності та стійкості системи до атак та технічних проблем.

Дана система, яка базується на блокчейні та технології Non-Fungible Tokens (NFT), пропонує ряд переваг, таких як децентралізоване сховище, збереження цілісності та доступності інформації, а також стійкість до несанкціонованих змін завдяки перевірці хешів. Однак, в роботі було виявлено деякі недоліки та проблеми, які потребують уваги:

- прозорість та відкритість блокчейну може призвести до аналізу мережі зловмисниками та можливості неправомірного доступу до даних. Рекомендується розглянути застосування інших типів блокчейну, таких як приватний або гібридний, для забезпечення керованого доступу до інформації та зменшення ризику несанкціонованого доступу;
- розділення системи на дві підсистеми, блокчейн та IPFS, може призвести до зниження рівня децентралізації та відкритості. Слід звернути увагу на можливість збереження даних відкритими, що може викликати неприйнятність для деяких сценаріїв використання;
- складність смарт-контрактів та витрати на їхнє розгортання можуть бути проблемою. Рекомендується розробка ефективних та мінімалістичних смарт-контрактів для забезпечення необхідного функціоналу, а додаткові функції винести за межі блокчейну;
- можлива втрата приватного ключа та недостатня захищеність мнемонічної фрази можуть призвести до втрати доступу до активів та конфіденційної інформації. Рекомендується розробка додаткових методів захисту та управління ключами для запобігання таким ситуаціям.

Отже, перед впровадженням системи на базі блокчейну та NFT слід уважно проаналізувати всі можливі ризики та розробити ефективні стратегії їх вирішення. Відповідно до цього, важливо продовжувати досліджувати та вдосконалювати технології для забезпечення найвищого рівня безпеки, ефективності та децентралізації, а також використання технологій блокчейну та NFT у державних реєстрах може мати значний потенціал для поліпшення управління даними та цифровими активами, але вимагатиме великих зусиль та співпраці для досягнення успіху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Behl, A., Pereira, V., Nigam, A., Wamba, S. & Sindhwani, R. (2024). Knowledge development in non-fungible tokens (NFT): a scoping review. *Journal of Knowledge Management, 28(1),* 232–267. https://doi.org/10.1108/JKM-12-2022-0937
2. AlKhader, W., Jayaraman, R., Salah, K., Sleptchenko, A., Antony, J. & Omar, M. (2023). Leveraging blockchain and NFTs for quality 4.0 implementation in digital manufacturing. *Journal of Manufacturing Technology Management, 34(7),* 1208–1234. https://doi.org/10.1108/JMTM-05-2023-0172
3. Chohan, U. W. (2021). Non-Fungible Tokens: Blockchains, Scarcity, and Value. *Critical Blockchain Research Initiative (CBRI) Working Papers.*
4. Dowling, M. M. (2021). Is Non-fungible Token Pricing Driven by Cryptocurrencies?

5. Kraken. (n. d.). *What are Non-Fungible Tokens? (NFT).* https://www.kraken.com/learn/what-are-non-fungible-tokens-nft
6. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
7. Dong, M., Wang, X., Niyato, D., & Han, Z. (2021). Blockchain for Secure and Trustworthy IoT: A Survey. *IEEE Access, 9*, 4955–4971. https://doi.org/10.1109/JIOT.2019.2920987
8. *The Certicom ECC Challenge.* (n. d.). https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html
9. Ajao, L. A., Agajo, J., Adedokun, E. A., & Karngong, L. (2019). Crypto hash algorithm-based blockchain technology for managing decentralized ledger databases. *J, 2(3),* 300–325. https://doi.org/10.3390/j2030021
10. Daniel, E., & Tschorsch, F. (2022). IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks, *IEEE Communications Surveys & Tutorials, 24(1),* 31–52. https://doi.org/10.1109/COMST.2022.3143147
11. Poberezhnyk, V., & Opirskyy, I. (2023). Development of the concept of the method of using blockchain technology for building a message exchange system. *Ukrainian Information Security Research Journal, 25(2),* 62–70. https://doi.org/10.18372/2410-7840.25.17673
12. *What is the InterPlanetary File System (IPFS), and how does it work?* (2023). https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work
13. *Mnemonic Phrase.* (2023). https://koinly.io/crypto-glossary/mnemonic-phrase/
14. Singh, P., & Singh, K. (2021). A review on security and privacy issues in blockchain technology. *Materials Today: Proceedings, 44,* 3495–3498. https://doi.org/0.1201/9781003022688-11

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Valeriia Balatska
PhD Students of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-6262-6792
valeriia.s.balatska@lpnu.ua

Vasyl Poberezhnyk
PhD Students of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-7523-2557
vasyl.poberezhnyk@gmail.com

Ivan Opirskyy
Doctor of Sciences, Professor, Professor of
Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

USE OF NON-FUNGIBLE TOKENS AND BLOCKCHAIN TO DEMARCATE ACCESS TO PUBLIC REGISTRIES

Abstract. In today's world, where digital technologies play an increasingly important role in various aspects of life, protecting data and ensuring its confidentiality and integrity is becoming an increasingly urgent task. This problem is especially important in the context of state registers, which contain a large volume of valuable information about citizens, businesses and other entities. Delimiting access to public registers is a key task for ensuring security, transparency and efficiency of data management in government bodies. In this context, the use of Non-Fungible Tokens (NFT) and blockchain technology can be a promising solution. This article examines the possibilities of using NFTs and blockchain to delimit access to public registries in Ukraine. This paper defines key concepts such as NFT, blockchain, identification, authentication, and access control and examines their possible applications for delimiting access to public registries. It also describes how the use of blockchain and NFT technologies can be a key solution for ensuring the security and efficiency of public registry management. Blockchain, as a distributed database, provides reliable storage of transaction history and impenetrable encryption of data. Each block in the chain has a unique hash that links it to the previous block, making any attempt to change the data in the blocks nearly impossible without detection. On the other hand, Non-Fungible Tokens (NFT) can serve as unique digital identifiers that define access rights to specific data in public registries. Each NFT contains a unique digital signature that confirms its ownership and characteristics, and can be used to precisely define access rights to specific data or resources. Together, these technologies can create a reliable and secure infrastructure for managing public registries, ensuring transparency, privacy and irreversibility of transactions.

Keywords: blockchain; Non-Fungible Tokens (NFT); authorization; identification; delimitation of access; decentralization.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Behl, A., Pereira, V., Nigam, A., Wamba, S. & Sindhwani, R. (2024). Knowledge development in non-fungible tokens (NFT): a scoping review. *Journal of Knowledge Management, 28(1),* 232–267. https://doi.org/10.1108/JKM-12-2022-0937
2. AlKhader, W., Jayaraman, R., Salah, K., Sleptchenko, A., Antony, J. & Omar, M. (2023). Leveraging blockchain and NFTs for quality 4.0 implementation in digital manufacturing. *Journal of Manufacturing Technology Management, 34(7),* 1208–1234. https://doi.org/10.1108/JMTM-05-2023-0172
3. Chohan, U. W. (2021). Non-Fungible Tokens: Blockchains, Scarcity, and Value. *Critical Blockchain Research Initiative (CBRI) Working Papers.*

4. Dowling, M. M. (2021). Is Non-fungible Token Pricing Driven by Cryptocurrencies?
5. Kraken. (n.d.). *What are Non-Fungible Tokens? (NFT).* https://www.kraken.com/learn/what-are-non-fungible-tokens-nft
6. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4,* 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
7. Dong, M., Wang, X., Niyato, D., & Han, Z. (2021). Blockchain for Secure and Trustworthy IoT: A Survey. *IEEE Access, 9,* 4955–4971. https://doi.org/10.1109/JIOT.2019.2920987
8. *The Certicom ECC Challenge.* (n. d.). https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html
9. Ajao, L. A., Agajo, J., Adedokun, E. A., & Karngong, L. (2019). Crypto hash algorithm-based blockchain technology for managing decentralized ledger databases. *J, 2(3),* 300–325. https://doi.org/10.3390/j2030021
10. Daniel, E., & Tschorsch, F. (2022). IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks, *IEEE Communications Surveys & Tutorials, 24(1),* 31–52. https://doi.org/10.1109/COMST.2022.3143147
11. Poberezhnyk, V., Opirskyy, I. (2023). Development of the concept of the method of using blockchain technology for building a message exchange system. *Ukrainian Information Security Research Journal, 25(2),* 62–70. https://doi.org/10.18372/2410-7840.25.17673
12. *What is the InterPlanetary File System (IPFS), and how does it work?* (2023). https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work
13. *Mnemonic Phrase.* (2023). https://koinly.io/crypto-glossary/mnemonic-phrase/
14. Singh, P., & Singh, K. (2021). A review on security and privacy issues in blockchain technology. *Materials Today: Proceedings, 44,* 3495–3498. https://doi.org/0.1201/9781003022688-11