УДК 62-50:004.942 DOI: 10.31673/2786-8362.2024.029628

Ізмалков О.М.

ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ ЯК ЗАСІБ ЗБЕРЕЖЕННЯ ДАНИХ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Izmalkov O.M. The use of smart contracts to store data in automated systems. This article is devoted to the study of the possibilities of implementing smart contracts as a means of ensuring data security in modern automated systems. In today's world, where digitalization covers all areas of activity, the problem of reliable data storage, protection and exchange is becoming increasingly relevant. Smart contracts, which are one of the key elements of blockchain technology, offer an innovative approach to solving these problems due to their transparency, process automation, and decentralization. This article analyzes the functionality of smart contracts, which allow for the automatic execution of agreements between the parties based on predefined conditions. These mechanisms significantly reduce the risks of data misuse and ensure their integrity and availability within the specified parameters. The main emphasis is placed on the integration of smart contracts with modern databases and cloud storage, which contributes to the efficiency of information management in automated systems

Keywords: smart contracts, blockchain, data storage, automated systems, information security

Ізмалков О.М. Використання смарт-контрактів як засіб збереження даних в автоматизованих системах. Смарт-контракти є новітньою технологією, яка дозволяє забезпечувати прозорість, безпеку та автоматизацію процесів у різних сферах діяльності. Використання смарт-контрактів у автоматизованих системах для збереження даних дає можливість мінімізувати ризики зловживання інформацією, а також гарантувати її цілісність і доступність. У статті розглядаються основні принципи роботи смарт-контрактів, їх переваги у сфері обробки даних, а також можливі сценарії застосування в автоматизованих системах. Запропоновані підходи до інтеграції смарт-контрактів з сучасними базами даних, які забезпечують високу ефективність і стійкість до зовнішніх впливів. Наведено аналіз перспектив застосування технології блокчейн для вирішення завдань у промислових, фінансових і медичних автоматизованих системах.

Ключові слова: смарт-контракти, блокчейн, збереження даних, автоматизовані системи, безпека інформації

Вступ

У сучасному світі автоматизовані системи набули широкого поширення в різних галузях, включаючи промисловість, медицину, фінансову сферу, логістику та державне управління. Їх основною метою є забезпечення швидкої та ефективної обробки великих обсягів інформації, що дозволяє автоматизувати процеси, зменшувати витрати, підвищувати продуктивність і забезпечувати високий рівень точності. Однак у міру зростання обсягу даних і складності цих систем постає низка викликів, пов’язаних із забезпеченням збереження, доступності, безпеки та цілісності даних.

Традиційні методи збереження даних, які базуються на централізованих базах даних і хмарних сховищах, часто виявляються вразливими до зовнішніх атак, втручань, збоїв у роботі інфраструктури чи людського фактору. З огляду на це, виникає необхідність пошуку нових, більш надійних підходів до зберігання даних. Одним із перспективних рішень цієї проблеми є використання блокчейн-технологій.

Блокчейн, як децентралізована система зберігання даних, забезпечує прозорість, стійкість до збоїв і підвищену безпеку. Інтеграція смарт-контрактів, що працюють на базі блокчейну, відкриває нові можливості для автоматизації управління даними. Смарт-контракти дозволяють виконувати операції в автоматичному режимі без необхідності посередництва, знижуючи ризики помилок і забезпечуючи виконання умов угод між сторонами.

Ці інноваційні технології мають потенціал для вирішення актуальних завдань, пов’язаних із забезпеченням надійного збереження та захисту даних. Вони знаходять застосування в таких сферах, як електронний документообіг, управління ланцюгами постачання, фінансові транзакції, медичні записи та багато інших.

Наукова новизна дослідження полягає в поєднанні сучасних технологій блокчейн і смарт-контрактів з традиційними методами збереження даних та їх адаптації для потреб конкретних галузей, що відкриває нові можливості для оптимізації управлінських процесів та забезпечення більш високого рівня безпеки і прозорості у збереженні даних. Особливістю роботи є інтеграція смарт-контрактів з існуючими базами даних і хмарними сховищами. В контексті даного дослідження розглядається можливість інтеграції технології смарт-контрактів з традиційними інформаційними інфраструктурами, що дозволяє автоматизувати процеси обробки і збереження даних без потреби повного переходу на нові технології. Це підвищує ефективність використання смарт-контрактів у вже існуючих системах і сприяє безшовній інтеграції з іншими технологіями.

Досліджено нові аспекти використання смарт-контрактів для забезпечення безпеки даних, зокрема на основі блокчейн-технологій, що гарантують стійкість до атак та зловживань, а також автоматизацію збереження даних з максимальним рівнем прозорості і недоступності для змін.

Здійснено аналіз застосування смарт-контрактів у специфічних галузях, таких як промисловість, фінанси, медицина та урядові структури, з урахуванням вимог до масштабованості, продуктивності та безпеки. Розглянуто, як саме технології блокчейн можуть оптимізувати процеси зберігання та обробки даних у кожній з цих галузей.

Аналіз і прогнозування ризиків, які можуть виникнути під час впровадження смарт-контрактів у традиційні системи. Для кожної з галузей було визначено конкретні проблеми, з якими можуть зіткнутися підприємства та установи при впровадженні смарт-контрактів, та розроблено рекомендації для їх подолання.

Аналіз останніх досліджень. Смарт-контракти, як ключовий компонент блокчейн-технології, є предметом активних досліджень і розробок. У своїй роботі Taherdoost (2023) детально аналізує концепцію смарт-контрактів, їхні технічні особливості та обмеження, зосереджуючись на критичному огляді існуючих підходів і реалізацій [1].

Perng та Chao (2021) досліджують впровадження смарт-контрактів у системи управління ланцюгами постачання, підкреслюючи можливості автоматизації процесів і забезпечення прозорості в бізнес-операціях [2]. Pustokhina (2021) вивчає їхній вплив на цифрову трансформацію у державному секторі, що є важливим для підвищення ефективності адміністративних процесів [3].

Питання безпеки смарт-контрактів також є ключовим аспектом досліджень. Delmolino (2021) у своїй роботі виявляють основні уразливості та ризики, пов’язані ізвикористанням смарт-контрактів, пропонуючи практичні рекомендації для їх усунення [4]. Zhang (2021) пропонують комплексний огляд питань безпеки та приватності у смарт контрактах, акцентуючи увагу на нових загрозах у сучасному середовищі.

Окремі роботи зосереджуються на галузевих застосуваннях. Chen та Zhang (2020) досліджують використання блокчейн-основи та смарт-контрактів для захисту медичних даних [6]. Роботи Antonopoulos та Wood (2021) спрямовані на розробку прикладних рішень для смарт-контрактів і децентралізованих додатків, що є корисними для технічної реалізації цих рішень [5]. Ghazal (2020) у своїх дослідженнях наголошує на використанні смарт-контрактів для забезпечення цілісності медичних даних [7].

Аналіз останніх досліджень вказує на значний потенціал смарт-контрактів у вирішенні завдань безпеки, прозорості та автоматизації процесів у різних галузях, водночас виділяючи проблеми, які потребують подальшого вирішення.

Постановка завдання. В межах дослідження були визначені основні завдання, спрямовані на глибоке вивчення проблем збереження даних та можливостей використання смарт-контрактів для їх ефективного та безпечного управління в автоматизованих системах. Основні задачі дослідження включають декілька завдань: аналіз існуючих підходів до збереження даних у автоматизованих системах та огляд сучасних методів збереження даних, таких як централізовані бази даних, хмарні сховища та традиційні технології зберігання.

Необхідно оцінити їхні переваги та обмеження, а також виявити основні проблеми, що виникають у процесі їх використання, зокрема щодо забезпечення безпеки, цілісності даних та їх доступності в умовах зростання обсягів інформації.

Завдання дослідження функціональних можливостей смарт-контрактів у контексті забезпечення безпеки даних полягає у вивченні особливостей смарт-контрактів, які працюють на базі блокчейн-технологій, і в їх здатності забезпечувати безпеку даних у реальному часі. Важливо розглянути, як смарт-контракти можуть автоматизувати процеси збереження та обміну даними, що дозволяє зменшити вплив людського фактору, підвищити прозорість операцій і забезпечити стійкість до зловмисних атак та технічних збоїв.

Розробка пропозицій щодо інтеграції смарт-контрактів із традиційними базами даних передбачає вивчення технічних аспектів і можливостей інтеграції смарт-контрактів із існуючими базами даних і хмарними сховищами. Метою є розробка рекомендацій для впровадження блокчейн-рішень у традиційні інформаційні інфраструктури з урахуванням специфіки галузей, вимог до масштабованості, продуктивності та безпеки.

Визначення переваг та ризиків використання смарт-контрактів у різних галузях вимагає провести оцінку потенційних переваг і недоліків використання смарт-контрактів у різних сферах діяльності, таких як промисловість, фінанси, медицина, урядові структури. Необхідно врахувати специфіку кожної галузі та визначити, як технології смарт-контрактів можуть оптимізувати процеси зберігання і обробки даних, а також знизити ризики, пов’язані з їх використанням. Особливу увагу буде приділено аналізу можливих загроз і технологічних обмежень, які можуть виникнути при їх впровадженні.

Метою роботи є дослідження можливостей застосування смарт-контрактів у сучасних автоматизованих системах для вирішення питань збереження даних. У роботі розглядаються технічні аспекти впровадження смарт-контрактів, аналізуються їх переваги та недоліки, а також перспективи інтеграції з існуючими інформаційними системами.

Особливу увагу приділено вивченню переваг використання децентралізованих технологій для забезпечення безпеки даних, аналізу потенційних ризиків та шляхів їхнього мінімізації. Очікується, що результати дослідження сприятимуть подальшому розвитку автоматизованих систем, підвищенню їхньої ефективності, адаптивності та надійності.

Виклад основного матеріалу дослідження.

Збереження даних є однією з основних складових будь-якої автоматизованої системи, оскільки від цього залежить не тільки ефективність роботи системи, але й забезпечення безпеки та цілісності інформації. У сучасних умовах, коли обсяги даних значно зросли, виникають нові виклики для збереження, обробки та передачі інформації. Основні підходи до збереження даних, централізовані бази даних, хмарні сховища та локальні або розподілені технології зберігання.

Централізовані бази даних традиційною технологією збереження даних, де інформація зберігається в одному місці – на сервері або в дата-центрі. Такі системи зазвичай використовують реляційні бази даних (RDBMS), які організовують дані у вигляді таблиць з фіксованими зв’язками між ними. Найпоширенішими базами даних такого типу є MySQL, PostgreSQL, Oracle.

Основні переваги: простота в управлінні: централізоване зберігання даних дозволяє зручніше здійснювати адміністрування та резервне копіювання. Адміністрація має можливість визначати, хто та як має доступ до даних, що підвищує рівень безпеки. Централізовані бази даних мають розвинуті інструменти для обробки великих обсягів інформації.

Основні обмеження це єдиний пункт відмови, оскільки вся інформація зберігається в одному місці, будь-який збій на сервері або в дата-центрі може призвести до втрати або тимчасового недоступності даних.

Хмарні сховища такі як Amazon S3, Google Cloud Storage або Microsoft Azure Storage, стають все більш популярними завдяки своїй гнучкості і можливості зберігати дані в

розподіленій мережі серверів. Дані зберігаються не на одному сервері, а в хмарі, доступ до якої можна отримати через інтернет. Хмарні сервіси дозволяють легко збільшувати обсяги збережених даних, забезпечуючи необхідний рівень продуктивності та зберігання без додаткових витрат на обладнання, надають доступ до даних з будь-якої точки світу, що особливо зручно для компаній, що працюють з віддаленими командами.

Хмарні сервіси автоматично забезпечують резервне копіювання та швидке відновлення даних у разі втрати.

Розподілені технології збереження даних такі як блокчейн, є інноваційним підходом до збереження та обміну даними. Блокчейн-технології дозволяють зберігати інформацію в мережі дистрибутивних вузлів, де кожен учасник має копію даних, що гарантує їхню незмінність і безпеку.

Основні переваги: безпека і незмінність даних: кожен блок у ланцюзі є криптографічно захищеним і не може бути змінений без згоди всіх учасників мережі.

Відсутність єдиного контролюючого органу зменшує ризики маніпуляцій та підвищує рівень довіри до збережених даних.

Усі зміни в даних реєструються та можуть бути перевірені учасниками, що забезпечує повну прозорість.

Особливості та обмеження технології: енерговитратність, особливо в разі використання таких алгоритмів, як Proof of Work (PoW), що потребує значних енергетичних ресурсів для підтвердження транзакцій. Через необхідність узгодження кожної транзакції між вузлами продуктивність блокчейн-систем може бути обмежена, що не підходить для деяких типів даних, що вимагають високої швидкості обробки.

Для реалізації та підтримки таких систем потрібні висококваліфіковані спеціалісти та інфраструктура.

Дослідження функціональних можливостей смарт-контрактів у контексті забезпечення безпеки даних. Смарт-контракти, як частина технології блокчейн, представляють собою програмні алгоритми, що автоматично виконують умови договору між сторонами без необхідності втручання посередників. Їх функціональність забезпечує не тільки автоматизацію бізнес-процесів, але й значно підвищує рівень безпеки при обміні та збереженні даних.

Основні особливості смарт-контрактів. Смарт-контракти дозволяють автоматично виконувати умови угоди, що означає зниження ризику помилок або маніпуляцій з боку користувачів. Це забезпечує високу точність та відповідність угодам.

Один з ключових аспектів, що підвищує безпеку даних – це незмінність інформації в блокчейні. Після того, як інформація була занесена до блокчейн-реєстру, її неможливо змінити або видалити. Це запобігає маніпуляціям з даними, навіть за наявності злому одного з учасників системи.

Завдяки дистрибуції даних по численних учасниках блокчейн-мережі, смарт-контракти знижують залежність від центральних органів або серверів. У разі збоїв або атак на одну точку мережі система продовжує функціонувати завдяки численним копіям даних на інших вузлах.

Блокчейн-технологія дозволяє забезпечити прозорість усіх операцій, що здійснюються через смарт-контракти. Кожен учасник має доступ до інформації про всі транзакції, що підвищує довіру до системи і знижує можливість шахрайства.

Забезпечення безпеки даних за допомогою смарт-контрактів:

Смарт-контракти можуть бути налаштовані таким чином, щоб доступ до даних мали лише авторизовані користувачі або організації. Завдяки криптографії і цифровим підписам смарт-контракти гарантують, що лише визначені сторони можуть змінювати дані або виконувати операції.

Страхування від помилок або спроб змінити умови: Усі умови угоди прописуються у коді смарт-контракту, що виключає вплив людського фактору або маніпуляції зі сторони

учасників. Смарт-контракт працює за чітко заданими умовами, що знижує ймовірність виникнення помилок у виконанні угод.

Смарт-контракти можуть бути доповнені різними механізмами безпеки, такими як двофакторна автентифікація, шифрування даних, а також методи перевірки цілісності даних, що дозволяє створювати надійні системи для обміну конфіденційною інформацією.

Смарт-контракти здатні значно підвищити стійкість до різних типів зловмисних атак. Оскільки блокчейн є дистрибутивною технологією, зловмиснику, навіть якщо йому вдасться зламати один із вузлів мережі, не вдасться змінити або скасувати умови смарт-контракту через необхідність досягнення консенсусу між усіма учасниками мережі.

В смарт-контрактах можуть бути реалізовані механізми для самоконтролю, перевірки умов виконання угоди. Якщо одна зі сторін намагається порушити умови або змінити дані, система автоматично зупиняє транзакцію та попереджає інших учасників. Це дозволяє знизити ризики шахрайства.

Математичне оцінка роботи смарт контрактів в автоматизованих системах. Смарт-контракт включає такі компоненти, як функції для взаємодії з користувачами, збереження даних, перевірка прав доступу та управління транзакціями. Основна програмна модель роботи смарт-контракту виконана на мові програмування solidity:

```
pragma solidity ^0.8.0;
contract SimpleStorage {
   // Змінна для збереження значення
   uint256 public storedData;

   // Подія для логування змін
   event DataStored(uint256 data);

   // Функція для збереження даних
   function set(uint256 x) public {
      storedData = x;
      emit DataStored(x); // Логування події
   }

   // Функція для отримання даних
   function get() public view returns (uint256) {
      return storedData;
   }
},
```

Де uint256 public *storedData*; – змінна для збереження даних, set(uint256 *x*) – функція, яка дозволяє зберігати значення в змінну *storedData* та емітувати подію *DataStored*, get() – Функція, яка повертає збережене значення та emit DataStored(*x*) – логування події для відслідковування змін у системі.

Принцип роботи:

1) Користувач викликає функцію set для того, щоб зберегти нові дані.
2) Система автоматично оновлює значення в змінній *storedData*.
3) Всі зміни фіксуються через події (emit), що дозволяє відслідковувати ці зміни в блокчейні.

Основна математична модель роботи смарт-контракту:

$$SC(t) = \begin{cases} 1, & \text{якщо } C_{in}(t) \to C_{out}(t), \\ 0, & \text{в іншому випадку,} \end{cases} \quad (1)$$

де:

- $SC(t)$ – результат виконання смарт-контракту в момент часу t (1 – успішне виконання, 0 – відмова);
- $C_{in}(t)$ – вхідні умови або параметри смарт-контракту в момент t;
- $C_{out}(t)$ – вихідні дані або результати роботи контракту.

Модель обчислення витрат:

Загальні транзакційні витрати на виконання смарт-контракту:

$$T_{cost}=T_{gas}+T_{storage} \quad (2)$$

де:

- T_{gas} – вартість виконання операцій контракту у вигляді спожитого “gas” в блокчейн мережі;
- $T_{storage}$ – вартість збереження даних у блокчейні.

Продуктивність і затримки. Середній час виконання смарт-контракту визначається за формулою

$$T_{exec}=T_{network}+T_{block}+T_{comp} \quad (3)$$

де:

- $T_{network}$ – час передачі даних між вузлами мережі;
- T_{block} – час генерації блоку у блокчейні;
- T_{comp} – час виконання обчислень на віртуальній машині.

Надійність імовірності помилок. Ймовірність успішного виконання контракту вимірюється за формулою:

$$P_{success}=1-P_{error}, \quad (4)$$

де:

- P_{error} – ймовірність помилки виконання та залежить від якості коду контракту, перевантаженості мережі, атак тощо.

Застосування моделі в автоматизованих системах. В автоматизованій системі у збереженні даних, смарт-контракти можна використовувати для автоматизації перевірки даних, умовного доступу до хмарного сховища, фіксації змін у даних у децентралізованому реєстрі.

Математична модель збереження даних. Обсяг даних, які потрібно зберегти, позначимо як D, а час доступу до них T. Вартість транзакції визначається за формулою:

$$C_{total}=T_{cost}+D*S_{cost} \quad (5)$$

де:

- S_{cost} – вартість одиниці збережених даних

Приклад автоматизованої системи. Система управління даними в ракетно-космічній техніці використовує смарт-контракт для перевірки прав доступу. Формула перевірки:

$$A_{access}(u,d)=\begin{cases}1, & \text{якщо } P(u)\wedge F(d),\\ 0, & \text{інакше,}\end{cases} \quad (6)$$

де:

- $A_{access}(u,d)$ – результат доступу користувача u до даних d;
- $P(u)$ – права користувача;
- $F(d)$ – стан даних d.

Описання та побудова смарт-контракту з урахуванням математичних функцій, інтегралів і умов. Функція збереження даних:

Нехай x – це значення, яке користувач хоче зберегти в системі через смарт-контракт. Смарт-контракт визначає функцію збереження даних, що записує x в змінну *storedData*, яка є частиною контракту. Тому збереження даних можна представити як функцію:

$$f_{store}(x)=storedData \text{ де } storedData=x, \quad (7)$$

це означає, що при виклику функції зберігання, значення *x* зберігається в контракті, а змінна *storedData* оновлюється до цього значення.

Функція доступу до даних. Функція доступу дозволяє користувачу отримати збережене значення *storedData*. Для цього смарт-контракт надає функцію доступу, що повертає значення *storedData*:

$$fget() = storedData, \tag{8}$$

кожен виклик функції $f_{get}()$ дає змогу отримати значення, що було раніше збережене в контракті.

Умова перевірки прав доступу. Якщо смарт-контракт передбачає перевірку прав доступу для виконання певних операцій, таких як збереження даних, тоді необхідно додати умову, що перевіряє ідентифікацію користувача. Наприклад, контракт дозволяє зберігати дані лише власнику:

$$\text{if } msg.sender=owner \text{ then } f_{store}(x), \tag{9}$$

msg.sender – це адреса користувача, який викликає функцію. *owner* – це адреса, яка має право на збереження даних. Умова визначає, що лише власник може зберігати дані, а інші користувачі отримують доступ до них лише для читання.

Подія (Логування зміни даних). Після того як дані зберігаються, смарт-контракт може генерувати подію для логування цієї зміни. Це подія фіксує факт зміни даних в блокчейн-мережі і забезпечує прозорість операцій. Формула події:

$$\text{emit DataStored}(x) \tag{10}$$

Подія DataStored записує значення *x* в реєстр подій, що може бути використано для аналізу або аудиту.

Інтеграція смарт-контракту з іншими функціями. Для більш складних смарт-контрактів можуть бути використані математичні функції, які дозволяють здійснювати обчислення або визначати динамічні зміни даних. Інтеграл може використовуватися для обчислення середнього значення з ряду даних, що зберігаються в контракті:

$$\int_a^b f(x)dx = \frac{1}{b-a}\sum_{i=1}^{n} xi \tag{11}$$

де *f*(*x*) – це функція, яка визначає зміну або модель даних, а *xi* – конкретні збережені значення. Таким чином, смарт-контракт може використовувати математичні методи для обробки і аналізу даних, забезпечуючи додаткові можливості для автоматизації та верифікації.

Умова виконання операцій. Смарт-контракт може виконувати певні операції, наприклад, змінювати значення, коли сума або середнє значення даних досягає певного порогу.

$$if \ \int_a^b f(x)dx \geq C \ then \ executive \ action \tag{12}$$

де *C* – це порогове значення, що визначає, коли має бути виконана дія.

Ця умова дозволяє смарт-контракту виконувати автоматичні операції на основі математичних розрахунків, що може бути корисно для систем, які працюють з великими обсягами даних.

Розширення: смарт-контракт з інтеграцією зовнішніх даних. Існують смарт-контракти, які інтегруються з зовнішніми джерелами даних, наприклад, через оракли (взаємодія з реальними даними поза блокчейном). *externalData*=oracleQuery(*request*), де oracleQuery(*request*) – це запит до оракла для отримання зовнішніх даних, які можуть використовуватися для подальших обчислень або збереження в контракті.

Основні аспекти інтеграції смарт-контрактів з традиційними базами даних.

- Вибір схеми інтеграції:

Гібридна модель дозволяє використовувати смарт-контракти для зберігання критичних або чутливих даних у блокчейні, а менш важливі дані – у традиційних базах даних або хмарних сховищах. Це дозволяє зберігати переваги децентралізованого зберігання без необхідності переносу всіх даних на блокчейн. При моделі з реєстрацією транзакцій бази даних зберігають лише частину інформації, а всі операції з даними (наприклад, зміни, оновлення) реєструються

в смарт-контрактах. Це дає змогу зберігати прозорість змін без необхідності зберігати всі дані в блокчейні.

- Масштабованість та продуктивність:

Традиційні бази даних, зокрема реляційні СУБД, добре справляються з великими обсягами даних, але блокчейн, зокрема через необхідність консенсусу в мережі, може обмежувати продуктивність. Для вирішення цього питання слід використовувати гібридні рішення, де смарт-контракти зберігають лише необхідну інформацію (наприклад, ідентифікатори записів або криптографічні хеші), а інші дані зберігаються в традиційних базах даних.

Смарт-контракти гарантують, що після їх запуску умови не можуть бути змінені, що забезпечує високий рівень безпеки для критичних даних. Для інтеграції з традиційними базами даних потрібно впровадити системи, які автоматично перевіряють відповідність даних у блокчейні та базі даних, запобігаючи можливим зловживанням або маніпуляціям.

Для забезпечення конфіденційності необхідно використовувати шифрування як у традиційних базах даних, так і в блокчейні, що дозволяє зберігати дані приватними навіть у відкритих мережах.

- Вимоги до консистентності даних:

Важливо забезпечити узгодженість даних між блокчейном і традиційними базами даних, особливо коли смарт-контракт змінює інформацію, яка зберігається в базі даних. Для цього можна використовувати оркестраційні інструменти, які синхронізують зміни між системами. Розробка API для взаємодії між традиційними базами даних і смарт-контрактами. API повинні забезпечувати безпечний обмін даними між блокчейном та базами даних, а також синхронізувати операції, які виконуються як на рівні блокчейну, так і в традиційних системах.

Традиційні бази даних можуть зберігати дані, що потребують високої швидкості доступу, в той час як блокчейн слід використовувати для зберігання метаданих, транзакцій або підтверджень. Системи для інтеграції повинні мати зручні API для роботи з базами даних та блокчейн-платформами. Це дозволить забезпечити двосторонню синхронізацію даних і гарантувати, що всі зміни в традиційних базах даних будуть автоматично відображені в блокчейні, і навпаки. Тестування і аудит безпеки проводиться перед впровадженням таких рішень потрібно проводити регулярні аудити смарт-контрактів і баз даних на наявність вразливостей, щоб забезпечити стійкість до атак і зловживань.

Визначення переваг та ризиків використання смарт-контрактів у різних галузях є важливим етапом у вивченні потенціалу цієї технології. Зважаючи на різноманітність галузей, в яких смарт-контракти можуть бути застосовані, їхня ефективність та застосовність безпосередньо залежить від специфіки кожної з них. Аналіз переваг і ризиків для основних галузей, таких як промисловість, фінанси, медицина та урядові структури.

Промисловість – основні переваги це автоматизація процесів, смарт-контракти дозволяють автоматизувати виробничі процеси, зокрема замовлення матеріалів, управління ланцюгами постачання та контролювання якості продукції. Це зменшує залежність від людського фактору і підвищує ефективність. Усі транзакції та операції можуть бути зафіксовані в блокчейні, що забезпечує прозорість та дає змогу відслідковувати кожен етап виробничого процесу. Використання смарт-контрактів дозволяє скоротити витрати на адміністрування, оскільки більшість операцій будуть автоматично виконуватись за заданими правилами.

Основні ризики впровадження смарт-контрактів у традиційні виробничі процеси це складна інтеграція та значні інвестиції а також нове програмне та апаратне забезпечення. Смарт-контракти мають обмеження по швидкості обробки даних, що може створити проблеми при великих обсягах інформації або високих вимогах до продуктивності.

В фінансовому секторі смарт-контракти знижують ризики шахрайства та помилок, оскільки всі угоди автоматично виконуються за заздалегідь визначеними умовами, що є публічно записані в блокчейні. Смарт-контракти дозволяють проводити фінансові транзакції

значно швидше і дешевше, ніж традиційні методи (банківські перекази, послуги фінансових посередників). Всі процеси, від підписання контрактів до виконання умов угод, можуть бути автоматизовані, що знижує кількість помилок і конфліктів між сторонами. Основні недоліки це відсутність єдиного правового регулювання для смарт-контрактів у багатьох країнах що створює ризики для учасників угод, вразливості в коді можуть містити програмні помилки або уразливості, що може призвести до фінансових втрат.

Переваги використання в медичній сфері це зберігання медичних записів з високим рівнем захисту завдяки шифруванню даних у блокчейні. Прозорість у взаємодії між учасниками дозволяє лікарям, пацієнтам та медичним установам здійснювати автоматизовані транзакції з обміну інформацією з гарантією її достовірності та цілісності. Процеси підтвердження медичних процедур, оплату послуг або перевірку наявності страховки, можуть бути автоматизовані.

Основні недоліки це складність правового регулювання, існують юридичні перешкоди для використання смарт-контрактів у медицині, оскільки ці технології ще не мають чітко визначеного правового статусу. Використання блокчейну для зберігання медичних даних може порушувати конфіденційність, якщо технологія не буде належно захищена.

В урядових структурах використання смарт-контрактів може значно підвищити рівень довіри громадян, оскільки всі операції будуть доступні для перевірки у публічному реєстрі. Автоматизація процедур видачі ліцензій, звітності, адміністрування державних програм може знизити навантаження на державні органи та підвищити ефективність управління.

Смарт-контракти мають значний потенціал для трансформації різних галузей завдяки підвищеній прозорості, автоматизації і зниженню витрат. Однак їх впровадження вимагає уважного підходу до безпеки, регулювання та інтеграції з існуючими системами. У кожній галузі потрібно враховувати специфіку та можливі ризики, такі як технічні обмеження, юридичні бар'єри та можливість зловживань, що може створити додаткові виклики для ефективного використання смарт-контрактів.

Висновки

Смарт-контракти представляють значний потенціал для удосконалення процесів зберігання та обробки даних у різних галузях, проте їх успішне впровадження потребує врахування специфіки та вимог кожної галузі, а також розв’язання потенційних технічних та безпекових викликів.

Використання смарт-контрактів у системах збереження даних дозволяє значно покращити їх безпеку, прозорість та цілісність. Завдяки автоматизації процесів обробки та зберігання інформації смарт-контракти мінімізують ризики, пов’язані з людським фактором, і знижують ймовірність помилок у даних.

Під час дослідження було виявлено, що інтеграція смарт-контрактів з існуючими базами даних і хмарними сховищами є перспективним напрямком для підвищення ефективності та безпеки існуючих інформаційних інфраструктур. Така інтеграція дозволяє зберегти переваги традиційних систем з урахуванням новітніх технологій, забезпечуючи надійність і масштабованість.

Використання смарт-контрактів у промисловості, фінансах, медицині та урядових структурах відкриває нові можливості для автоматизації зберігання та обробки даних. Особливо важливою є здатність блокчейн-технологій забезпечити децентралізацію, що підвищує рівень довіри до обробки інформації.

Важливо враховувати можливі технологічні обмеження, такі як низька пропускна здатність мережі або висока вартість транзакцій, що можуть обмежити широке застосування в певних галузях. Також важливо забезпечити високий рівень захисту від потенційних атак або зловмисних маніпуляцій.

Розвиток технології блокчейн і смарт-контрактів продовжує активно просуватися, і в майбутньому можна очікувати вдосконалення цієї технології, що дозволить підвищити її

продуктивність, знизити витрати на використання та вирішити проблеми, пов'язані з масштабованістю.

Для ефективного впровадження смарт-контрактів в автоматизовані системи необхідно проводити глибоке тестування та адаптацію технологій до специфіки кожної галузі. Необхідно розробити стратегії щодо подолання можливих технічних та безпекових ризиків, що можуть виникнути під час інтеграції новітніх технологій у традиційні інфраструктури.

Список використаної літератури:

1.Taherdoost H. Smart Contracts in Blockchain Technology: A Critical Review. Information. 2023. Vol. 14, no. 2. P. 117. URL: https://doi.org/10.3390/info14020117.

2. High-G Shock Reliability of 3-D Integrated Structure Microsystem Based on Finite Element Simulation / Y. Long et al. IEEE Transactions on Components, Packaging and Manufacturing Technology. 2021. Vol. 11, no. 8. P. 1243–1249. URL: https://doi.org/10.1109/tcpmt.2021.3094594

3. Tan E., Mahula S., Crompvoets J. Blockchain governance in the public sector: a conceptual framework for public management. Government information quarterly. 2021. P. 101625. URL: https://doi.org/10.1016/j.giq.2021.101625.

4. Guo H., Yu X. A survey on blockchain technology and its security. Blockchain: research and applications. 2022. P. 100067. URL: https://doi.org/10.1016/j.bcra.2022.100067

5.Antonopoulos, A., & Wood, G. (2021). Mastering Ethereum: Building Smart Contracts and Dapps. O'Reilly Media.

6.Blockchain for healthcare systems: architecture, security challenges, trends and future directions / A. J et al. Journal of network and computer applications. 2023. Vol. 215. P. 103633. URL: https://doi.org/10.1016/j.jnca.2023.103633.

7. Uni-OPU: An FPGA-Based Uniform Accelerator for Convolutional and Transposed Convolutional Networks / Y. Yu et al. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 2020. Vol. 28, no. 7. P. 1545–1556. URL: https://doi.org/10.1109/tvlsi.2020.2995741.

Автор статті

Ізмалков Олексій – старший викладач, Дніпровський національний університет імені Олеся Гончара, Дніпро, Україна.

ORCID: 0009-0005-3732-7474

Author of the article

Izmalkov Oleksii – senior lecturer, Oles Honchar Dnipro National University, Dnipro, Ukraine.

ORCID: 0009-0005-3732-7474