DOI: 10.58254/viti.6.2024.07.93

УДК: 004.056

Куцаєв П. В. ORCID: 0000-0002-3235-3316 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Данилюк І. А. ORCID: 0000-0002-7192-9242 (ВІТІ ім. Героїв Крут)
Паламарчук С. А. ORCID: 0000-0001-7483-9165 (ВІТІ ім. Героїв Крут)
Чередниченко О. Ю. ORCID: 0000-0002-0816-8321 (ВІТІ ім. Героїв Крут)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПОТРЕБ СЕКТОРА БЕЗПЕКИ І ОБОРОНИ

Блокчейн-технології швидко завойовують популярність у різних галузях завдяки своїй здатності забезпечувати надійний захист даних, прозорість та децентралізацію. Особливо важливими вони стають у сфері телекомунікацій, де зберігання, обробка, передача та управління даними має критичне значення, особливо у військовій сфері. Використання технології блокчейн може значно підвищити рівень безпеки, ефективність та надійність в зазначеній галузі, вирішуючи проблеми централізації та вразливості до атак.

Використання блокчейн-технологій, за рахунок їх децентралізації, значно підвищить безпеку інформаційно-комунікаційних систем, завдяки розподіленій архітектурі, де дані зберігаються на численних незалежних вузлах, що ускладнює їхнє масове знищення чи модифікацію. Відсутність єдиної точки відмови знижує ризики зламів, а механізми консенсусу забезпечують перевірку і захист від несанкціонованих змін. В цілому, така технологія дозволяє створювати більш стійкі, надійні та захищені системи, що дозволить значно зменшити втрати особового складу, техніки та майна.

Метою дослідження є аналіз сучасного стану та існуючих проблемних питань, які автори пропонують вирішити за допомогою розробки та впровадження блокчейн-технологій у телекомунікаційній галузі, зокрема білінгових операцій, роумінгу, управління ідентифікацією користувачів та дослідження можливостей автоматизації процесів за допомогою смарт-контрактів, що дозволить підвищити ефективність роботи інформаційно-комунікаційних систем за рахунок підвищення швидкості передачі даних і оптимізації їх роботи.

Подальші наукові дослідження, на думку авторів, можуть бути спрямовані на можливість масштабування та зниження енергоспоживання використання технології блокчейн, а також на його інтеграцію з іншими технологіями, такими як штучний інтелект та квантові технології.

Ключові слова: *блокчейн, телекомунікації, безпека даних, смарт-контракти, автоматизація, білінг, роумінг.*

P. Kutsaiev, I. Danyliuk, S. Palamarchuk, O. Cherednychenko Prospects of using blockchain technology in the field of information protection in state institutions

Blockchain technologies are rapidly gaining popularity in various industries due to their ability to provide reliable data protection, transparency and decentralization. They become especially important in the telecommunications, where the storage, processing, transmission and management of data are of critical importance, especially the military industry. The implementation of blockchain technology can significantly increase the level of security, efficiency and reliability in the mentioned industry, solving the problems of centralization and vulnerability to attacks.

The use of blockchain technologies, due to their decentralization, will significantly increase the security of information and communication systems, due to the distributed architecture, where data is stored on numerous independent nodes, which makes their mass destruction or modification difficult. The absence of a single point of failure reduces the risks of breaches, and consensus mechanisms provide verification and protection against unauthorized changes. In general, this technology allows for the creation of more stable, reliable and protected systems, which will significantly reduce the loss of personnel, equipment and property.

The purpose of this scientific researching is to analyze the current state and existing problematic issues, which the authors propose to solve with the help of the development and implementation of blockchain technologies in the telecommunications industry, in particular, billing operations, roaming, user identity management, and the researching of the possibilities of automating processes using smart contracts, which will allow to increase the efficiency of information and communication systems, due to increasing the speed of data transmission and optimizing their work.

Further scientific research, according to the authors, can be aimed at the possibility of scaling and reducing energy consumption of the using of blockchain technology, as well as its integration with other technologies, such as artificial intelligence and quantum technologies.

Keywords: *blockchain, telecommunications, data security, smart contracts, automation, billing, roaming.*

Постановка проблеми. У сучасному світі, де дані стають одним з основних засобів у сучасних військових конфліктах, питання їхньої захищеності набувають особливої актуальності. Інформаційно-психологічні операції, крадіжки даних і шахрайство стають щоденними викликами для різних сфер. Технологічні рішення, що базуються на централізованих системах зберігання, стають все менш ефективними для протидії цим загрозам.

У традиційних централізованих системах безпеки даних операції часто перевіряються і підтверджуються центральними серверами або адміністраторами, що може стати потенційною вразливістю, особливо в умовах зростання обсягів даних та цифровізації суспільства. Такі галузі, як державні структури, сили оборони, засоби масової інформації, телекомунікації, фінанси та охорона здоров’я, потребують надійних рішень для забезпечення захисту даних та автоматизації процесів.

Аналіз останніх досліджень. Технологія блокчейн, вперше запропонована у 2008 році Сатоші Накамото для використання у криптовалюті Bitcoin, виявила свій потенціал далеко за межами фінансового сектора. В її основі лежить розподілений реєстр, який зберігає дані у вигляді послідовних блоків, що додаються до ланцюжка, утворюючи своєрідну цифрову книгу, де кожна зміна фіксується і доступна для всіх учасників системи. Це робить блокчейн надзвичайно привабливим для галузей, де потрібно забезпечити незмінність і цілісність інформації, а також прозорість транзакцій між різними сторонами [1].

Останні дослідження підтверджують, що використання блокчейн-технологій стає важливим інструментом для підвищення безпеки інформації в різних галузях, включаючи телекомунікації, фінанси та різноманітні процеси в урядових структурах. Наприклад, автори [5] зазначають, що блокчейн-технологія суттєво спрощує процеси автоматизації та забезпечення безпеки у телекомунікаціях, зокрема через впровадження смарт-контрактів. Саме впровадження блокчейн-технологій підвищує автоматизацію білінгових операцій і роумінгу, що значно підвищує прозорість і надійність транзакцій між операторами зв’язку [2].

Дослідження [6] фокусується на викликах та можливостях впровадження блокчейн-технологій у телекомунікаціях. Вони зазначають, що основними перевагами блокчейн є його здатність захищати ідентифікаційні дані користувачів і запобігати шахрайству. Смарт-контракти дозволяють автоматизувати процеси перевірки ідентичності, що суттєво знижує ризики компрометації даних під час обробки транзакцій [3].

Огляд досліджень, проведений авторами [7], зосереджується на інформаційно-комунікаційних системах із застосуванням блокчейн-технологій для захисту транзакцій і передачі даних. Проведене дослідження свідчить про те, що блокчейн-технологія підвищує ефективність управління мережею та здійснює контроль доступом до ресурсів через децентралізовану платформу. Це відкриває можливості для впровадження блокчейн-технологій не лише в галузі телекомунікацій, але й в інших галузях, таких як фінансові послуги, побутова сфера та охорона здоров’я.

Блокчейн-технології також привертають увагу дослідників у сфері кібербезпеки. Автори [8] у своїх дослідженнях підкреслюють, що основними перевагами блокчейн-технології – є захист даних від модифікацій і фальсифікацій. Вони зазначають, що криптографічні алгоритми, такі як хеш-функція, забезпечують незмінність інформації, що робить використання блокчейн-технологій надійним рішенням для зберігання чутливої інформації.

Крім того, автори [9] провели дослідження економічних аспектів щодо використання блокчейн-технологій. Вони дійшли висновку, що блокчейн-технологія дозволяє знизити витрати на зберігання даних та обробку транзакцій завдяки автоматизації операційних процесів. Їхні дослідження свідчать, що компанії, які використовують блокчейн, досягають вищої стабільності та рентабельності.

Таким чином, аналіз досліджень підтверджує значні переваги блокчейн-технологій для безпеки даних, зниження витрат та підвищення ефективності роботи в різних галузях. Проте, як зазначається у дослідженнях, блокчейн-технологія також стикається з викликами, такими як високе енергоспоживання та проблеми масштабування, що потребує подальших досліджень та вдосконалень [2, 3].

Метою даного дослідження є аналіз сучасного стану та існуючих проблемних питань, які автори пропонують вирішити за допомогою розробки та впровадження блокчейн-технологій у телекомунікаційній галузі, зокрема білінгових операцій, роумінгу, управління ідентифікацією користувачів, та дослідження можливостей автоматизації процесів за допомогою смарт-контрактів, що дозволить підвищити ефективність роботи інформаційно-комунікаційних систем, за рахунок підвищення швидкості передачі даних і оптимізації їх роботи.

Виклад основного матеріалу дослідження. Блокчейн – це децентралізована база даних, яка зберігає записи (блоки) інформації у вигляді послідовного ланцюга. Кожен блок містить хеш попереднього блоку, що робить ланцюг незмінним після додавання нових блоків. Головною особливістю блокчейн є його незмінність, завдяки тому, що будь-які спроби змінити дані у вже створеному блоці призводять до того, що всі попередні блоки цього ланцюга мають бути також змінені, що виявляє фальсифікацію при такій спробі. Це можливо завдяки тому, що всі вузли мережі мають копії всіх блоків, що гарантує високий рівень безпеки.

Блокчейн використовує криптографічні алгоритми для забезпечення захисту даних. Одним з основних механізмів є хеш-функція, яка генерує унікальний цифровий підпис для кожного блоку даних. Цей цифровий підпис неможливо відтворити, що робить фальсифікацію практично неможливою. Кожен новий блок додається до ланцюжка з хешем попереднього блоку, і навіть мінімальні зміни у даних призведуть до зміни хеш-функції, що буде негайно виявлено іншими учасниками мережі.

Крім того, блокчейн підтримує розподілене зберігання даних, де інформація зберігається на всіх вузлах мережі одночасно. Це означає, що навіть якщо один вузол мережі виходить з ладу, дані залишаються доступними для всіх інших учасників. Це суттєво підвищує надійність і стійкість мережі, оскільки втрата або знищення даних на одному вузлі не призведе до втрати інформації.

Ще одним ключовим елементом блокчейн є алгоритми консенсусу, які дозволяють учасникам мережі домовлятися про додавання нових блоків без необхідності у централізованому управлінні. Найпоширенішими алгоритмами консенсусу є Proof of Work (PoW) та Proof of Stake (PoS)**.** Алгоритм PoW передбачає вирішення складних математичних задач, що потребує великих обчислювальних ресурсів. PoS, у свою чергу, дозволяє учасникам мережі валідувати нові блоки, базуючись на їхньому вкладі (стейку) у систему, що зменшує енергоспоживання та збільшує швидкість транзакцій [1, 4].

Смарт-контракти – ще один спосіб використання технології блокчейн, який дозволяє автоматизувати виконання зобов'язань між учасниками договору за попередніми домовленостями, які унеможливлюють випадки шахрайства, будь-ким, в тому числі і членів угоди. Це спеціальні програми, на основі блокчейн-технології, які автоматично виконують умови угоди, щойно всі необхідні параметри виконані.

Наприклад, смарт-контракт може визначити, які дані доступні певному підрозділу на основі його рівня доступу або функціональних обов'язків. При цьому всі дії фіксуються в блокчейн, та будь-яка зміна доступу або перегляд інформації записується для подальшої перевірки. На рис. 1 зображена модель смарт-контракту, який визначає чи має право доступу підрозділ оборони А та В до інформації в блоках.

Рис. 1. Спрощена модель опису функціонування смарт-контракту

Смарт-контракти значно підвищують ефективність транзакцій та усувають необхідність у третіх сторонах, що часто є джерелом затримок та додаткових витрат [1].

Використання блокчейн-технологій у сфері телекомунікацій може суттєво підвищити рівень безпеки даних та автоматизації операційних процесів. Запропонований підхід передбачає впровадження систем на основі блокчейн-технологій для управління доступом, білінгом, роумінгом та ідентифікацією користувачів, що допоможе забезпечити вищу прозорість і стійкість до кібератак.

1. Управління доступом: блокчейн-технології можуть використовуватися для управління доступом до інформації між підрозділами сектора безпеки і оборони завдяки своїй децентралізованій архітектурі і криптографічним методам захисту даних. У такій системі всі операції з даними реєструються у блокчейні, і кожен підрозділ отримує доступ тільки до тієї інформації, яка йому необхідна для виконання своїх завдань. Використання смарт-контрактів дозволяє автоматично надавати або обмежувати доступ до певних даних відповідно до рівня доступу кожного підрозділу. Наприклад, рій БпЛА, який функціонує під управлінням одного блокчейн, може безперервно відображати обстановку в заданому секторі, розпізнавати об’єкти та приймати рішення про приналежність об’єкта ворогу, а далі надавати доступ до даних тільки визначеним підрозділам, тим самим підтримуючи ситуаційну обізнаність для всіх учасників бойових дій [15]. На рисунку 2 представлена методика з використанням блокчейн-технології для виявлення ворожих об’єктів на полі бою.

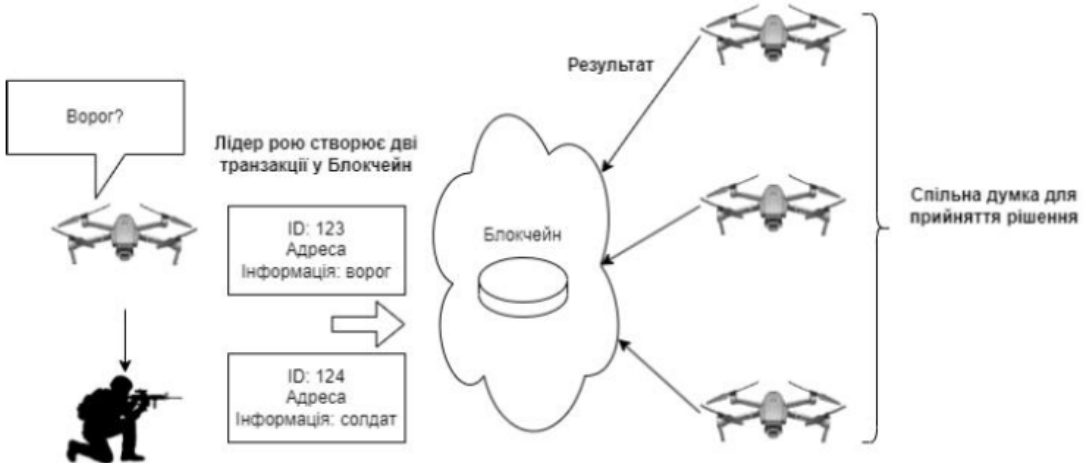

Рис. 2. Методика з використанням блокчейн-технологій для виявлення ворожих об’єктів на полі бою

Децентралізоване зберігання даних: дані зберігаються в розподіленій мережі, що складається з ланцюга блоків, кожен з яких захищений криптографічними алгоритмами. Кожен запит на доступ до інформації записується у блок, і всі вузли ланцюга можуть перевірити легітимність цього запиту. Наприклад, у випадку захоплення ворогом певного пристрою, при спробі підключитись до блокчейну він буде заблокований, оскільки інші учасники будуть попереджені про втрату пристрою. Це запобігає несанкціонованим спробам доступу до інформації.

Шифрування даних: кожен блок у ланцюжку даних шифрується за допомогою криптографічних методів, що дозволяє зберігати дані у незмінному вигляді і забезпечити їхню конфіденційність. Доступ до блоків можливий лише через розшифровку з використанням приватних ключів, що надаються виключно авторизованим користувачам.

Математична модель **контролю за доступом** до інформації між підрозділами базується на розрахунку рівня авторизації доступів до інформації для кожного підрозділу.

Контроль за доступом для підрозділу Ci можна розрахувати як співвідношення кількості успішних доступів до загальної кількості спроб доступу для кожного підрозділу згідно виразу (1):

$$Ci = \frac{n_{auth}(i)}{n_{total}(i)}, \tag{1}$$

де $n_{auth}(i)$ – кількість авторизованих доступів підрозділу i;

$n_{total}(i)$ – загальна кількість спроб доступу підрозділу i.

Вираз (1) дозволяє оцінити, наскільки успішно підрозділ здійснює доступ до інформації. Якщо $Ci \approx 1$, це означає, що всі спроби доступу були авторизованими, що свідчить про високий рівень контролю за доступом.

Показник Ci може бути оптимізований за допомогою: використання смарт-контрактів для автоматичного управління доступом, додаткового шифрування ідентифікаційних даних користувачів для перевірки їх рівня доступу.

Загальний рівень захищеності військових комунікацій S можна оцінити через сукупність контрольованого доступу до інформації по всіх підрозділах згідно виразу (2):

$$S = \frac{\sum_{i=1}^{N} C_i A_i}{\sum_{i=1}^{N} A_i}, \tag{2}$$

де N – кількість підрозділів ;

Ci – контроль за доступом для підрозділу i;

Ai – вага або важливість інформації для підрозділу i.

Вираз (2) дозволяє оцінити загальний рівень захищеності мережі, враховуючи як ефективність контролю за доступом до інформації, так і важливість даних, до яких мають доступ підрозділи. Якщо деякі підрозділи мають високий рівень доступу до критично важливих даних, це підвищує загальну вразливість системи, тому слід зосередити ресурси на забезпеченні їх захищеності.

Для підвищення захищеності комунікацій потрібно: збільшити рівень авторизованих доступів $n_{auth}(i)$; впровадити більш ефективні криптографічні механізми для перевірки ідентифікації користувачів; використовувати смарт-контракти для автоматизації процесу контролю доступу.

Оскільки військові комунікації можуть постійно змінюватись (нові підрозділи, змінюється кількість спроб доступу до даних), можна враховувати динаміку зміни рівня захищеності згідно з виразом (3):

$$S(t) = \frac{\sum_{i=1}^{N} C_i(t) A_i}{\sum_{i=1}^{N} A_i}, \tag{3}$$

де t – час надання доступу.

Вираз (3) дозволяє аналізувати, як захищеність змінюється з часом, виявляти підрозділи, які можуть ставати більш вразливими, та швидко реагувати на зміни.

2. Управління білінгом та роумінгом через смарт-контракти: традиційні білінгові системи телекомунікаційних компаній мають певні вразливості, зокрема щодо прозорості розрахунків між операторами. У випадку роумінгу, це може бути досить складний процес, який включає взаємодію різних систем і операторів для правильного розподілу витрат і наданих послуг. Наприклад, під час спільних навчань на території країн-партнерів, потрібно відпрацьовувати розгортання різних типів зв’язку з різними операторами. Застосування блокчейн-технології може стати вирішенням цієї проблеми за рахунок впровадження смарт-контрактів. У випадку з роумінгом, смарт-контракти можуть автоматично розраховувати платежі між операторами на основі фактичного використання послуг (рисунок 3), знижуючи ризик помилок або шахрайства. Це також прискорить процес білінгу, оскільки операції автоматизуються та виконуються майже миттєво [3, 4].

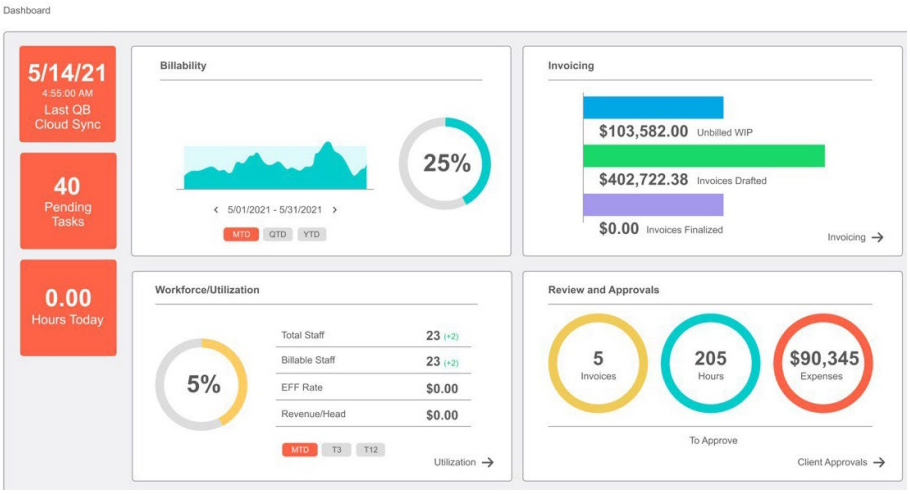

Рис. 3. Автоматичний розрахунок вартості наданих послуг

Смарт-контракти можуть також допомогти вирішити проблеми з оптимізацією білінгу для сил безпеки і оборони (рисунок 4). Замість того, щоб оператори вручну відстежували використання послуг кожного підрозділу та складали рахунки, смарт-контракти можуть автоматично фіксувати всі операції у реальному часі, зберігаючи їх у блокчейні.

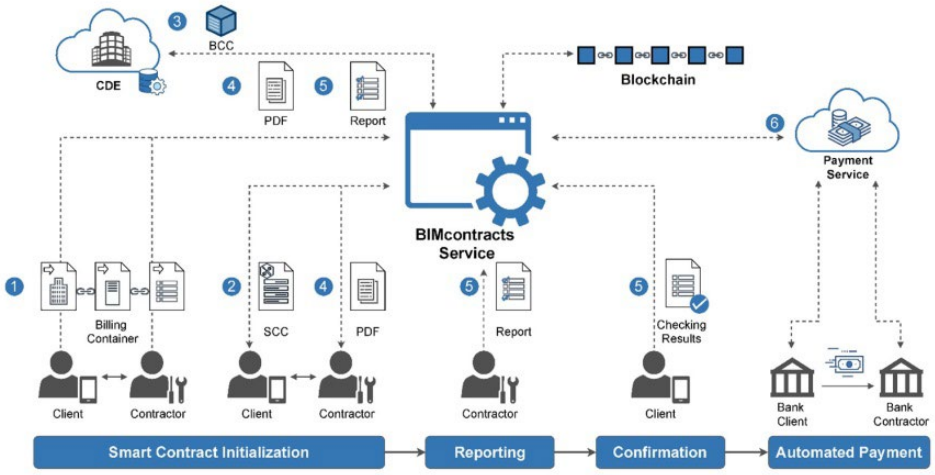

Рис. 4. Схема білінгу для сил безпеки і оборони

Підрозділи можуть мати доступ до детальної інформації про всі свої витрати, що підвищує рівень довіри та прозорості між користувачем і оператором зв'язку [1, 3].

3. Управління ідентифікацією та забезпечення конфіденційності даних: управління персональними даними та ідентифікацією користувачів є однією з найважливіших задач у телекомунікаційних мережах. Використання блокчейн-технологій дозволяє підвищити безпеку цієї інформації через децентралізоване зберігання та криптографічний захист даних. Кожен користувач може мати свій унікальний ідентифікатор, зберігаючи його у блокчейні, що знижує ймовірність несанкціонованого доступу або крадіжки ідентифікаційних даних [1].

Крім того, блокчейн дозволяє користувачам мати контроль над своїми даними. Це означає, що лише користувач може вирішувати, кому надавати доступ до своїх персональних даних, і будь-яка зміна або доступ до цих даних буде зафіксована у блокчейні, забезпечуючи повну прозорість і захист конфіденційності. Цей підхід допомагає вирішити проблеми шахрайства з ідентифікацією та значно знижує ризики витоку даних.

Переваги блокчейн-технології:

1. **Децентралізація**: однією з головних переваг блокчейн є децентралізована архітектура, яка усуває необхідність у довірених третіх сторонах. У традиційних системах безпеки дані, зазвичай, зберігаються на центральних серверах, що створює єдину точку відмови та робить систему вразливою до атак. У блокчейн дані зберігаються на кожному вузлі мережі, і кожен учасник має свою копію всіх транзакцій. Це підвищує стійкість системи до атак, оскільки для модифікації даних необхідно змінити всі копії у всіх вузлах, що майже неможливо. Така децентралізація забезпечує високий рівень **захисту від зовнішніх атак**, зокрема DDoS, та мінімізує ризики внутрішніх загроз.

2. **Прозорість та незмінність даних**: усі транзакції, що зберігаються в блокчейн, прозорі та незмінні. Це означає, що кожна зміна даних фіксується і відразу стає доступною для всіх учасників мережі. Ця властивість робить блокчейн особливо корисним у галузях, де важливо забезпечити довіру між сторонами, наприклад, у фінансових операціях або державних послугах. Крім того, оскільки дані не можуть бути змінені без узгодження з усіма учасниками мережі, це запобігає шахрайству та маніпуляціям [1]. Прозорість блокчейн також дає можливість відслідковувати походження продуктів або транзакцій, що особливо корисно для управління ланцюгами постачання [3].

3. **Підвищення ефективності та автоматизація**: завдяки впровадженню смарт-контрактів блокчейн дозволяє автоматизувати операційні-процеси, які традиційно вимагали участі третіх сторін або ручної перевірки. Використання смарт-контрактів значно знижує витрати на управління операціями та підвищує швидкість їх виконання. На рисунку 5 зображено середній час на виконання операцій з використанням блокчейн-технології та з використанням традиційних баз даних [16].

Впровадження блокчейн-технологій вимагає значного часу на налаштування системи, інтеграцію з існуючими процесами та навчання персоналу. Згідно виразу (4) можливо оцінити ефективність впровадження блокчейн-технологій у телекомунікаційні мережі з точки зору **приведеного витраченого часу** $NPV_{\text{час}}$.

$$NPV_{\text{час}} = \sum_{t=1}^{T} \frac{CF_t}{(1+r)^t} - I_0, \quad (4)$$

де: $NPV_{\text{час}}$ – приведений витрачений час;

I_0– початкові інвестиції у часі (в середньому оцінюється в 2000 год);

CF_t – щорічна економія часу;

r– ставка дисконтування часу (5% (0.05), що відображає зменшення цінності часу з кожним роком через інші задачі, що потребують уваги).

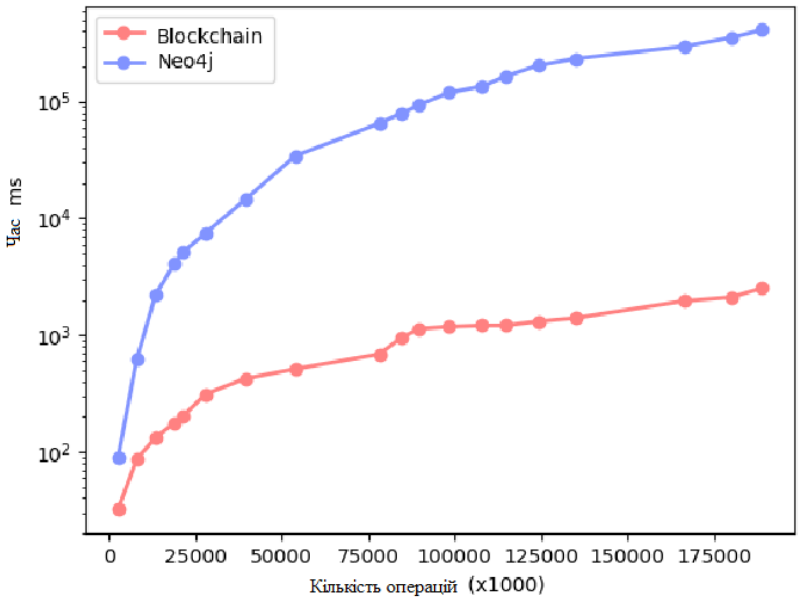

Рис. 5. Середній час виконання запиту для баз даних Neo4j
та при застосуванні блокчейн-технології

Розрахуємо дисконтовану економію часу для першого року згідно виразу (4).

$$\frac{CF_t}{(1+r)^t} = \frac{500}{(1+0.05)^1} = 476.19 \text{ год.}$$

У таблиці 1 наведено приклад розрахунку $NPV_{\text{час}}$ для 5 років.

Таблиця 1

Розрахунок приведеного витраченого часу $NPV_{\text{час}}$

Рік (t)	**Економія часу CF_t, год**	**Дисконтована економія часу $\frac{CF_t}{(1+r)^t}$, год**
1	500	476.19
2	700	635.27
3	800	691.14
4	900	739.39
5	1000	783.53
Разом		3325.52

Загальний $NPV_{\text{час}} = 3325.52 - 2000 = 1325.52$ год

Позитивне значення $NPV_{\text{час}}$ у часі (1325.52 годин) показує, що впровадження блокчейн-технологій у телекомунікаційні мережі дозволяє зекономити значну кількість робочих годин протягом 5 років, що робить впровадження технології ефективним.

4. **Безпека та захист від модифікацій** забезпечується хеш-функціями.

5. **Інтеграція з іншими технологіями для покращення захисту:** використання блокчейн-технологій може бути інтегровано з іншими передовими технологіями, такими як штучний інтелект (ШІ) та квантові технології, наприклад, криптографія з використанням постквантових алгоритмів, для створення більш комплексної системи безпеки. Використання ШІ, для моніторингу транзакцій у блокчейн, дозволить виявляти підозрілі активності та аномалії в реальному часі, що підвищить рівень безпеки мережі. Наприклад, ШІ може аналізувати поведінку користувачів і виявляти будь-які відхилення від нормального патерну, сигналізуючи про можливі втрати пристроїв під час бойових дій або наявність вірусних програм на них.

Квантова криптографія, яка використовує принципи квантової механіки для забезпечення найвищого рівня безпеки, також може бути інтегрована з блокчейн-технологіями. Це дозволить захистити дані навіть від найскладніших, на сьогодні, атак, що можливо тільки при використанні квантових комп'ютерів. Квантова криптографія може значно покращити рівень захисту персональних даних, зберігаючи їх недоступними для зловмисників навіть у майбутніх високотехнологічних атаках.

6. **Підвищення ефективності за допомогою токенізації та децентралізованого управління даними:** однією з новітніх тенденцій у телекомунікаціях є впровадження токенізації, що дозволяє операторам створювати цифрові токени для керування різними активами та послугами. Токенізація на основі блокчейн-технологій може бути використана для надання підрозділам сил оборони доступу до певних послуг або ресурсів, а також для управління використання програмного забезпечення.

Обмеження блокчейн-технології:

1. **Високе енергоспоживання**: одним з найбільших викликів, пов'язаних з використанням блокчейн-технологій, є високе енергоспоживання, особливо у випадку використання алгоритму **Proof of Work (PoW)**, який використовується у таких мережах, як Bitcoin. PoW вимагає значних обчислювальних ресурсів для вирішення складних математичних задач, що підтверджують нові блоки. Це призводить до великих витрат електроенергії, що робить блокчейн менш екологічно чистим рішенням порівняно з традиційними централізованими системами. Наприклад, мережа Bitcoin споживає більше електроенергії, ніж деякі країни, що викликає занепокоєння щодо стійкості цієї технології [1, 2].

2. **Проблеми масштабованості**: іншою значною проблемою блокчейн є його обмежені можливості для масштабування. Оскільки кожна транзакція має бути підтверджена всіма учасниками мережі, це суттєво знижує швидкість обробки даних. Це особливо актуально для мереж, які використовують PoW, де обробка транзакцій може займати кілька хвилин або навіть годин. У таких секторах, як телекомунікації або фінанси, де потрібна висока пропускна здатність, блокчейн може виявитися менш ефективним рішенням [2]. Проте нові алгоритми консенсусу, такі як **Proof of Stake (PoS)**, дозволяють знизити ці проблеми, забезпечуючи вищу швидкість транзакцій та знижуючи енергоспоживання.

3. **Складність інтеграції з існуючими системами**: впровадження блокчейн технологій у вже існуючі централізовані системи може бути досить складним і витратним процесом. Багато держаних структур стикаються з проблемами під час інтеграції блокчейн з наявними ІТ-системами через відмінності в архітектурі та принципах роботи. Це може вимагати значних інвестицій у перепроєктування інфраструктури та навчання співробітників для роботи з новою технологією.

4. **Правові та регуляторні бар'єри**: блокчейн, як і багато інших новітніх технологій, стикається з правовими та регуляторними викликами. Багато країн ще не розробили чітке законодавство, яке б регулювало використання блокчейн-технологій, особливо у сферах оборони, фінансів та обміну даними. Це створює додаткові ризики для державних органів, що планують впровадження цієї технології, оскільки вони можуть стикнутися з правовими обмеженнями або невизначеністю щодо її легальності [4].

Висновки. Проведене дослідження, на думку авторів, свідчить, що використання блокчейн-технологій мають величезний потенціал у забезпеченні безпеки даних у різних галузях, таких як телекомунікація, логістика, проєктування, моніторинг, фінанси, структури державних установ та інші. Блокчейн-технології надають унікальні можливості завдяки своїм властивостям децентралізації, прозорості та цілісності інформації. Ці властивості роблять блокчейн одним із найперспективніших технологічних рішень для боротьби з основними

проблемами сучасних централізованих систем, такими як наявність єдиної точки відмови, недостатня прозорість операцій та високі ризики витоку даних.

Особливо важливими виявляються можливості впровадження блокчейн в інформаційно-комунікаційних системах, де виникає потреба у підвищенні прозорості білінгових операцій, автоматизації процесів роумінгу та управлінні ідентифікаційними даними користувачів. Використання смарт-контрактів дозволяє спростити та прискорити ці процеси, забезпечуючи водночас надійний захист даних і зниження витрат на управління. Це відкриває нові горизонти для підвищення ефективності управління, покращуючи взаємодію між операторами та користувачами.

Блокчейн-технологія також виявляє себе як потужний інструмент для захисту інформації, у таких галузях, як оборона, проєктування, охорона здоров'я та фінансові послуги. Завдяки децентралізованому зберіганню та криптографічним механізмам захисту, блокчейн дозволяє значно знизити ризики витоків інформації та атак на системи зберігання даних. Цю технологію, на думку авторів, доцільно використовувати для управління медичними записами під час військово-лікарської комісії, де повинна забезпечуватися повна прозорість і контроль з боку військовослужбовців над своїми персональними даними.

Незважаючи на значні переваги, блокчейн-технологія має свої обмеження, зокрема пов'язані з проблемами масштабованості та енергоспоживання. Алгоритми консенсусу, такі як Proof of Work (PoW), потребують значних обчислювальних ресурсів для підтримки функціонування мережі, що може стати перешкодою для широкого впровадження блокчейн в системах, де потрібно швидко обробляти великі обсяги даних. Однак нові алгоритми, такі як Proof of Stake (PoS), дозволяють знизити ці обмеження та підвищити ефективність обробки транзакцій, що робить блокчейн більш придатним для комерційного використання.

Перспективи подальших досліджень. Подальші дослідження у сфері розвитку та впровадження блокчейн-технологій, на думку авторів, можуть бути спрямовані на вирішення проблем, пов'язаних з можливістю масштабування та зниження енергоспоживання. Нові алгоритми консенсусу, такі як PoS, PoC (Proof of Capacity) та PoA (Proof of Authority), можуть суттєво покращити продуктивність при застосуванні блокчейн-технологій, що забезпечить водночас високу швидкість транзакцій та низькі витрати на енергоспоживання.

Ще одним перспективним напрямком подальшого розвитку та впровадження блокчейн-технологій може бути інтеграція блокчейн-технологій з іншими передовими технологіями, такими як штучний інтелект (ШІ) та квантова криптографія. Використання ШІ для моніторингу транзакцій у блокчейн може суттєво підвищити рівень захисту мережі, виявляючи аномалії та потенційні загрози в режимі реального часу.

Криптографія, з використанням постквантових алгоритмів, може суттєво підвищити рівень безпеки блокчейн, забезпечуючи захист даних навіть від потенційних загроз, які можуть виникнути з розвитком квантових комп'ютерів. Інтеграція зазначеної технології дозволить створити більш стійкі та безпечні системи для зберігання та обробки даних, що відкриває нові можливості для широкого впровадження блокчейн у майбутньому.

Ще одним важливим напрямом для подальших досліджень автори вважають розробку нормативно-правової бази на державному рівні, що дозволить здійснювати регулювання використання блокчейн-технологій. У багатьох країнах відсутнє чітке регулювання цієї технології, що може стримувати її впровадження на державному рівні та у великих структурах, таких як Збройні Сили України. Розробка нормативно-правової бази, що враховує особливості використання блокчейн-технологій, допоможе знизити правові ризики та сприятиме подальшому поширенню цієї технології для підвищення ефективності функціонування багатьох галузей.

Блокчейн-технологія може запропонувати революційні можливості для **покращення управління логістикою** в ЗСУ, забезпечуючи прозорість та незмінність усіх операцій,

пов'язаних з постачанням техніки, озброєння та матеріалів. Децентралізована система дозволяє зберігати всі транзакції, пов'язані з постачаннями, у вигляді блоків, що гарантує відсутність фальсифікацій або втручань ззовні. Кожна логістична операція реєструється в блокчейні, що дозволяє легко відстежувати будь-яку військову техніку та її стан на будь-якому етапі транспортування або експлуатації.

Використання смарт-контрактів у логістиці дозволяє автоматизувати виконання угод щодо постачання, знижуючи ризики людських помилок та забезпечуючи своєчасність поставок.

Блокчейн-технологія може також бути використана для **моніторингу технічного обслуговування** військової техніки та обладнання. Автоматизована система, на базі блокчейн-технології, дозволить в реальному часі відстежувати стан техніки, що забезпечить підвищення оперативності та забезпечить своєчасність її обслуговування. Кожна операція з технічного обслуговування буде зареєстрована у ланцюжку блокчейн цієї системи, що забезпечить доступ до інформації необхідного персоналу для та оптимізації процесів ремонту та технічного обслуговування.

Під час **проєктування військових систем** (наприклад, систем озброєння або IT-інфраструктури), блокчейн може забезпечити координацію між різними учасниками проєкту (підрядниками та військовими структурами). Це дозволить вести точний облік внесків кожного із учасників, відслідковувати зміни та оновлення при виконанні проєкту. Блокчейн-технологія може бути використана для забезпечення безпеки використання та зберігання даних, що критично важливо при розробці нових технологій, де потрібно уникнути витоків або шахрайства.

Таким чином, впровадження блокчейн-технологій мають потенціал стати основним інструментом для забезпечення безпеки даних і автоматизації операційних процесів у багатьох галузях. Однак, для якісного та ефективного впровадження блокчейн-технологій необхідні подальші дослідження у вирішенні проблемних питань, що на даний час існують при використанні блокчейн-технологій щодо масштабованості, енергетичної ефективності, інтеграції з іншими технологіями та розробки відповідних нормативно-правової законодавчої бази.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Blockchain Technology Review. 2023. URL: https:// ar5iv.labs.arxiv.org/blockchain-review.

2. Blockchain in Telecommunications: Challenges and Opportunities. MDPI Journals. 2022. URL: https://www. MDPI.com/journal/blockchain-telecom.

3. Understanding Blockchain Technology. 2023. URL: https://Reintech.io/blog/understanding-blockchain.

4. Arthur D. Little. How blockchain platforms enhance telecom & media. ADL Insights. 2022. URL: https://www.adlittle.com/blockchain-telecom-media.

5. Zhang, X., Li, J., Wang, Y. Blockchain technology in telecommunications: a review. Journal of Network and Computer Applications. 2022. URL: https://www.journal.com/blockchain-telecommunications-review.

6. Liu, S., Zhao, Q., Chen, R. Application of Blockchain in Telecommunications: Challenges and Opportunities. Telecommunications Policy. 2022. URL: https://www.telecompolicy.org/blockchain-challenges-opportunities.

7. Мануілов Я. С. Використання технології блокчейн у телекомунікаціях // Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71), № 3. С. 123–127. DOI: https://doi.org/10.32838/2663-5941/2021.3/20.

8. Четверіков І. О., Петренко А. І. Впровадження блокчейн для забезпечення інформаційної безпеки // Журнал кібербезпеки. 2021. № 99. С. 162–169. DOI: 10.33111/mise.99.

9. Койбічук В. В., Рожкова М. С. Економічний аналіз використання блокчейн у різних галузях. Науковий журнал економічних досліджень. 2021.

10. Nazanin Moosavi, Hamed Taherdoost. Blockchain Technology Application in Security: A Systematic Review. MDPI, 2023. P. 60-=–70. URL: https://doi.org/10.3390/blockchains1020005.

11. Sparsh Sharma, Imtiaz Ahmad, Shaima Qureshi, Malik Ishfaq. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 2022. URL: https://www.mdpi.com/fi14110341.

12. Daneshgar F, Ameri Sianaki O, Guruwacharya P. Blockchain: a research framework for data security and privacy. In Advances in Intelligent Systems Computing. 2019. URL: https://doi.org/10.1007/978-3-030-15035-8_95.

13. Banchhor P, Sahu D, Mishra A, Ahmed MB. A systematic review on blockchain security attacks, challenges and issues. IJERT, 2021. URL: https://www.ijert.org/research/a-systematic-review-on-blockchain-security-attacks-challenges-and-issues-IJERTV10IS040292.pdf.

14. Krishnan KN, Jenu R, Joseph T, Silpa ML. Blockchain based security framework for IoT implementations. IEEE, 2018. URL: https://doi.org/10.1109/CETIC4.2018.8531042.

15. Опірський І., Василишин С. Перспективи військового застосування технології блокчейну // Ukrainian Scientific Journal of Information Security. 2022. Т. 28, № 2. С. 57–66. DOI: 10.18372/2225-5036.28.16950.

16. Tsoulias K., Palaiokrassas G., Fragkos G., Litke A., Varvarigou T. A graph model-based blockchain implementation for increasing performance and security in decentralized ledger systems // IEEE Access. 2020. DOI: 10.1109/ACCESS.2020.3006383.