

**Мануїлов Я.С.**Український науково-дослідний інститут спеціальної техніки та судових експертиз  
Служби безпеки України

## ВИКОРИСТАННЯ ТЕХНОЛОГІЇ «БЛОКЧЕЙН» У ТЕЛЕКОМУНІКАЦІЯХ

У статті розглядається особливості технології «блокчейн» (*block chain* з англійської — ланцюжок блоків), її переваги та недоліки, можливості використання у телекомунікаційних системах, наданні послуг операторами на базі даної технології. Прозорість та гнучкість проведення банківських, фінансових та іншого виду операцій з використанням технології блокчейн. Ведення публічних реєстрів з історією, яку не можна змінити, проведення онлайн голосувань, системи цифрового посвідчення осіб та нотаріату. Довіра до систем побудованих на базі технології блокчейн заснована на чіткому виконанні усіма учасниками, децентралізованої системи, встановлених у алгоритмах роботи правил та перевірки виконання цих правил кожним з учасників. Навіть якщо зловмисник спробує провести помилкову, хибну операцію, кожний учасник мережі автоматично за допомогою програмного забезпечення перевірить валідність даної операції та відкине її як помилкову. Розглядається стійкість до відмов розподілених телекомунікаційних систем побудованих з використанням технології блокчейн. Використання смарт-контрактів (розумних контрактів) при наданні різного виду телекомунікаційних послуг. Принципи доступності та незмінності інформації, прозорості при виконанні транзакцій та обслуговуванні блокчейн систем у телекомунікаціях. Проводиться аналіз ефективності та доцільності використання технології блокчейн у телекомунікаційних системах. Розглядаються можливості використання даної технології для оптимізації бізнес-процесів у компаніях, які надають телекомунікаційні послуги та у банківському секторі. Застосування нових віртуальних ідентифікаторів абонентів, що обслуговуються, замість морально застарілих, дозволить спростити обслуговування абонентів, роумінгові угоди між операторами та створити можливості для нових видів послуг. Здійснюється розгляд математичного (криптографічного) підґрунтя технології блокчейн, що базується на хеш-функції та цифровому підписі, які гарантують цілісність та незмінність інформації та механізм перевірки володіння без необхідності звернення до арбітра. Можливості та складності, які можуть виникнути під час впровадження технології блокчейн у наявні телекомунікаційні системи.

**Ключові слова:** блокчейн, транзакції, хеш-функція, цифровий підпис, децентралізовані мережі, смарт-контракти, телекомунікаційні послуги.

**Постановка проблеми.** На сучасному етапі розвитку суспільства відбувається бурхливий розвиток інформаційно-телекомунікаційних систем і технологій і, як результат, їх широке використання в різних секторах суспільства. Значна кількість сучасних державних та приватних установ використовують інформаційні та телекомунікаційні системи для управління виробничими процесами, підтримки рішень, зберігання та обробки інформації, пошуку необхідних даних та багато іншого.

Конфіденційність, безпека, надійність, цілісність переданої інформації між різними користувачами системи останнім часом вимагає широкої уваги з боку фахівців у галузі розвитку телекомунікаційних мереж. Особливо актуальним є момент передачі конфіденційних даних щодо відкриття доступу до захищених банківських профілів клієнтів. Водночас наявні алгоритми захисту, політика їх використання не завжди можуть бути

гарантом від сторонніх мережевих атак, тоді як реалізація виділеного підключення може бути непрактичною і фізично не реалізованою з урахуванням особливостей функціонування телекомунікаційних мереж [3].

Блокчейн-технології, протоколи та архітектура як окрема реалізація нової інформаційної системи можуть бути взяті за основу в процесі створення нової захищеної системи передачі та обміну даними.

**Постановка завдання.** Розгляд технології блокчейн, її структури, визначення особливостей захисту даних, особливо при реалізації відомого на сьогодні алгоритму видобутку, може бути використане в процесі створення вдосконаленого прототипу банківської системи розрахунків, де основною складовою передачі даних є транзакція.

З іншого боку, ресурси біткойн-платіжної системи можуть стати поштовхом для переоснащення наявних телекомунікаційних мереж

з позиції забезпечення в останніх широкого розгалуження, підвищеної безпеки даних у критичних вузлах та чіткої прозорості при доступі інформаційні ресурси мережі. Таке рішення в рамках дослідження було обрано із принципу, що саме в технології блокчейн можна відстежувати та передбачати всі дії щодо передачі даних завдяки логічно побудованій та добре організованій архітектурі зв'язку кінцевих вузлів.

Майже всі ці системи працюють за принципом централізованого управління процесом, а повний контроль над системою може бути досягнутий за допомогою доступу до центрального головного сервера. У результаті збільшується ризик пошкодження всієї системи, збільшується кількість вразливостей та загроз для ІТС.

**Виклад основного матеріалу.** Зважаючи на суспільний інтерес до технології блокчейн та її активне використання в різних сферах, таких як фінанси та бухгалтерський облік, доцільно проаналізувати ефективність даної технології у телекомунікаціях. Своєю назвою «Blockchain» частково характеризує принцип самої технології. «block» – це блок, «chain» – це ланцюжок. Звідси випливає, що блокчейн – це ланцюжок блоків.

Блокчейн підтримує суворий порядок, визначений складними криптографічними функціями. Блоки – це дані про транзакції, угоди та контракти в системі, які представлені в криптографічній формі. Всі блоки розташовані в ланцюжку, тобто з'єднані послідовно. Щоб додати (записати) новий блок, потрібно перевірити порядок попередніх блоків.

Розглянемо уважніше на роботу системи блокчейн. Кожен блок або запис у реєстрі блокчейн містить основну інформацію, обчислює власний хеш попереднього блоку. Набір даних, що зберігається в блоці, залежить від призначення блокчейну. Наприклад, блокчейн біткойн містить інформацію про відправника, одержувача та кількість перерахованих монет. Хеш кожного блоку унікальний, як і дані, що зберігаються в блоці. Його унікальність можна порівняти з відбитком пальця людини. Якщо ви внесете, навіть незначні, зміни до блоку, хеш блоку зміниться. Третім елементом блоку є хеш попереднього блоку. Таким чином формується послідовність блоків. Ця модель робить блокчейн безпечним.

Мережа блокчейнів добре справляється із підтримкою цілісності даних. Через наявність багатьох копій бази даних та їх змін лише після підтвердження правильності інформації іншими учасниками мережі інформація залишається захищеною від навмисних, несанкціонованих або

випадкових змін, а також від змін під час зберігання або передачі.

Інформацію більше не можна змінювати через технічні помилки в роботі мережевого вузла або через людський фактор, оскільки підтвердження операцій базується на складних математичних функціях. Це означає, що інформація залишається незмінною та правильною. Забезпечення цієї категорії інформаційної безпеки гарантує стабільну роботу, правильні рішення та можливість зберігати дані, як вони були створені [4].

Відповідно до принципу доступності інформація повинна бути доступна уповноваженим особам у потрібний час. У мережі блокчейнів кожен учасник вважається авторизованим і може в будь-який час читати або писати дані та брати участь у верифікації даних, доданих іншими учасниками. Конфіденційність інформації досягається наданням доступу з найменшими дозволами, тобто уповноважена особа повинна мати доступ лише до даних, визначених для її прав доступу.

Будь-який учасник мережі може викликати повну копію бази даних на своєму пристрої та прочитати всі дані, що містяться в ній, що принципово суперечить принципу конфіденційності даних. Зберігання даних у базі блокчейн в зашифрованому вигляді принципово не вирішує проблему конфіденційності, оскільки конфіденційні дані, такі як особисті дані, в більшості випадків не втрачають своєї актуальності з часом. Дешифрування отриманих даних є питанням часу і залежить від обчислювальної потужності зловмисника, який намагається отримати доступ до інформації.

Телекомунікації – це неймовірно складна галузь, яка вимагає величезної фізичної інфраструктури, складних мереж з багатьма учасниками, складних систем виставлення рахунків, роумінгових угод та інших аспектів. Упровадження технології блокчейн може здатися досить складним кроком у цій багаторівневій галузі, але насправді впровадження розподіленої книги та інтелектуальних контрактів допоможе значно спростити всі бізнес-процеси телекомунікаційної компанії.

Телекомунікаційні компанії пов'язують людей один з одним через телефони та Інтернет по кабелю або по бездротовому зв'язку. Індустрія телекомунікацій виявляється застарілою, оскільки вона заснована на картах модулю ідентифікації абонента (SIM), які були розроблені ще в 1991 році. Доброю новиною є те, що SIM-карти поступово замінюються картами eSIM, які являють собою цифровий чіп, який робить ту ж роботу.

Але недостатньо просто задовольнятися зручною і швидкою установкою плат нового покоління, і тому оператори звертаються до технології блокчейн, яка знає, як правильно обробляти дані. Blockchain – це база даних, яка підтримує постійно зростаючий набір даних.

Зараз Blockchain – одна з найбільш широко обговорюваних та відкритих технологій. Ця технологія несе в собі можливість зруйнувати бізнес-моделі в багатьох галузях, включаючи телекомунікації, і може підвищити прозорість та ефективність процесу. Великою перевагою blockchain є те, що він є загальнодоступним. Усі учасники можуть бачити блоки та транзакції, що зберігаються в них. Це не означає, що кожен може бачити фактичний зміст транзакції; він захищений вашим приватним ключем [1].

Телекомунікаційний ланцюжок створення вартості складається із забезпечення необхідної мережевої інфраструктури та підключення для передачі голосу, даних, мультимедіа та інших супутніх послуг. Обмін даними відбувається між мережами, що вимагає захисту даних, цілісності даних, перевірки даних та запобігання шахрайству.

Технологія Blockchain пропонує телекомунікаційній галузі ідеальне рішення для однієї з основних вимог. Завдяки надійному безпечному доступу до даних блокчейн вже використовується в багатьох додатках у телекомунікаційній галузі. Можливість зберігати історичні записи користувачів без можливості втручання в ці записи дозволяє контролювати різні аспекти облікових записів користувачів. Деякі блокчейн-додатки в телекомунікаційній галузі включають автоматизацію багатьох внутрішніх операцій, таких як системи виставлення рахунків, роумінг та управління ланцюгами поставок.

Автоматизація білінгових систем за допомогою смарт-контрактів, що надаються за допомогою технології блокчейн, економить компанії багато часу та грошей та запобігає будь-якій можливості шахрайства. Як результат, весь процес бухгалтерського обліку та аудиту буде автоматизований, що дозволить заощадити телекомунікаційним компаніям більше грошей [3].

З'являються нові варіанти управління мережею та нові моделі спільного використання інфраструктури, такі як управління орендою сегментів мережі 5G для телекомунікаційних компаній та мережевих партнерів, підприємств, операторів мобільних віртуальних мереж (MVNO – mobile virtual network operator) та гравців Over the Top (OTT). Блокчейн може допомогти спростити процес обслугову-

вання, зробити його безпечним, прозорим та ефективним, а також знайти нові потоки доходу за допомогою пропозицій щодо цифрового пакету.

Технологія блокчейн все ще має величезний потенціал, щоб завоювати телекомунікаційну індустрію. Пакет послуг на основі блокчейн може створити нові потоки доходу для телекомунікаційних компаній. Незважаючи на те, що ці послуги ще не повністю вивчені або виявлені, деякі з них вже досить зрозумілі, щоб їх можна було широко застосовувати.

Низька вартість використання блокчейн для дешевих платежів може дозволити телекомунікаційним компаніям надавати мікроплатежі, які зазвичай використовуються для купівлі мобільних онлайн-ігор, музики тощо. У результаті розгортання цієї послуги стороннім додаткам не потрібно надавати реквізити банківського рахунку, дані кредитної картки чи будь-яку іншу конфіденційну чи конфіденційну інформацію. Іншими словами, блокчейн-додатки в телекомунікаційній галузі забезпечать ще більш високий рівень безпеки для користувачів телекомунікацій.

Ідея використання методу обліку та відстеження, який захищає від фальсифікації чи захисту, робить додатки блокчейн безмежними на всіх ринках, що вимагають безпеки. Більшість програм, що використовують технологію блокчейн у телекомунікаціях, є фінансовими тим чи іншим чином.

Спрощення фінансових операцій та переказів із використанням технології блокчейн обіцяє перенести телекомунікаційні компанії в майбутнє, коли ці компанії стануть повністю функціональними банками з мінімально можливою вартістю. Цей крок буде посилений тим фактом, що телекомунікації є однією з галузей, яка користується високим рівнем довіри споживачів. Використання програм, заснованих на блокчейні, посилить цю довіру і одночасно посилить її.

Блокчейн слід сприймати як нову технологічну парадигму. Технологія збрала кілька концептуально різних ідей. Такі галузі, як розподілені реєстри пам'яті, алгоритми консенсусу та криптографічні механізми захисту даних, були об'єднані. Багато аспектів технології блокчейн раніше активно обговорювались і просувались як окремі рішення в технологічних колах. Блокчейн – це логіка зберігання, яка не залежить від централізованого сервера або групи серверів [1].

Замість того, щоб звертатися до третіх осіб, таких як фінансові установи, як посередники у транзакціях, вузли мережі блокчейнів використовують спеціальний консенсус-протокол для

узгодження вмісту книги, а також криптографічні алгоритми хешування та цифрові підписи для забезпечення цілісності транзакції та передачі її параметрів.

Механізм консенсусу гарантує, що розподілені книги є точними копіями, що зменшує ризик шахрайських транзакцій, оскільки сторонні втручання можуть виникати в багатьох місцях одночасно. Криптографічні алгоритми хешування, такі як алгоритм обчислення SHA256, гарантують, що будь-яка зміна вхідних даних транзакції, навіть найменша, призведе до різного хеш-значення в результатах обчислення, що вказує на те, що вхідні дані транзакції можуть бути скомпрометовані. Цифрові підписи гарантують, що транзакції здійснюються законними відправниками (підписаними приватними ключами), а не зловмисниками.

Децентралізована однорангова мережа блокчейн позбавляє окремих учасників або групи учасників можливості контролювати базову інфраструктуру або дестабілізувати всю систему. Усі учасники мережі рівні і підключаються до неї за допомогою однакових протоколів. Учасниками можуть бути приватні особи, державні установи, організації чи асоціації всіх перелічених типів учасників.

По суті, система фіксує хронологічний порядок транзакцій з усіма вузлами в мережі, які визнали дійсність транзакцій через обрану модель консенсусу. Результатом є транзакції, які не можна скасувати або змінити.

Технологія формує та зберігає список упорядкованих записів, які називаються блоками. Кожен блок містить мітку часу і, що дуже важливо, унікальний образ (хеш) попереднього блоку, таким чином технологія «з'єднує» блоки даних, виключаючи можливість зміни даних у сформованих блоках без зміни всієї послідовності. Завдяки уніфікації технологічних рішень блокчейн має кілька вражаючих відмінних рис: відкритість, незмінність збережених даних, а також можливість публікувати та керувати виконуваною логікою (програмним кодом) у децентралізованій мережі. Усі ці аспекти роблять блокчейн цікавою та перспективною технологією [4].

У традиційних комерційних мережах усі учасники надають підтримку власним дублікатам книг, розбіжності між якими призводять до суперечок, збільшують час врегулювання, а також вимагають залучення посередників з усіма супутніми витратами. Водночас використання розподілених книг, заснованих на технології блокчейн, в яких транзакції не можуть бути змінені після прийняття консенсусу та внесення їх у книгу, може заоща-

дити підприємцям час і гроші, а також зменшити можливі ризики.

Технології блокчейн обіцяють більшу прозорість взаємодії між зацікавленими сторонами, вдосконалену автоматизацію, адаптацію реєстрів до індивідуальних вимог, а також вищий рівень довіри до ведення діловодства. Механізми консенсусу в блокчейні мають переваги консолідованого та упорядкованого набору даних, який має менше упереджень та квазіреальних довідкових даних і дозволяє учасникам вносити зміни в описи своїх активів.

Оскільки жоден учасник не володіє центральним джерелом походження інформації, що міститься в розподіленій книзі, технології блокчейн підвищують рівень довіри та забезпечують цілісність інформаційного потоку між учасниками.

Незмінність механізмів блокчейну призводить до зниження витрат на аудит та підвищення прозорості дотримання нормативних актів. І оскільки контракти, укладені в комерційних мережах, що базуються на технології блокчейн, є розумними, автоматизованими та остаточними, бізнес виграє від високої швидкості виконання, зменшення витрат та ризиків та своєчасного врегулювання контрактів [2].

Технологія блокчейн, завдяки своїм відмінним особливостям, пропонує позбутися «зайвої ланки» (арбітра) у більшості бізнес-процесів і може взяти на себе ролі, традиційно важливі у секторі фінансових послуг. Розумні контракти, засновані на децентралізованій виконуваний логіці, можуть бути корисними і поза фінансовим сектором.

Можливість укладання контрактів, параметризованих за допомогою зовнішніх потоків даних (ціни акцій, звіти про погоду, заголовки новин) і укладених сторонами на основі електронного блокчейну, змінює середовище ведення бізнесу майже у всіх галузях: «8% з 3000 опитаних організацій в різних країнах світу перейшли на пілотну стадію або на стадію впровадження технології блокчейн. У даний час 25% вивчають можливість впровадження у найближчі 12 місяців. Серед них – фінансові компанії – 33%, державний сектор – 29%, охорона здоров'я – 27%.

Технологія блокчейн може кардинально змінити класичні бізнес-процеси. Цю технологію можна використовувати для створення захищених від фальсифікацій систем голосування, створення реєстрів незмінної історії накопичення даних та багато іншого [3].

Варто зазначити, що в гонитві за сенсацією та революцією багато людей концентруються на перевагах технологій. Блокчейн не слід сприймати

як технологію, яка може вирішити будь-яку проблему. Через використання консенсусних алгоритмів та використання об'ємних математичних розрахунків та розподіленої логіки зберігання даних більшість систем блокчейн не мають високої швидкості обробки транзакцій. Таким чином, під час автоматизації процесів та побудови інформаційних систем з використанням технології блокчейн необхідно чітко розуміти, яке конкретне завдання вирішує блокчейн, яку оптимізацію процесу та які переваги він приносить.

**Висновки.** Отже, технологія блокчейн досі вважається відносно новою. Ось чому в ньому так багато нерозкритих можливостей. Завдяки технології блокчейн світ зараз перебуває у фазі створення нового інструменту, який можна використовувати так, про який ніхто інший не знає. Цифрові телекомунікаційні компанії прагнуть до інформатизації всієї організації та екосистем, і блокчейн може бути життєздатним рішенням для конкретних сценаріїв та забезпечити спрощений процес, ефективність та прозорість.

### Список літератури:

1. Blockchain architecture basics: components, structure, benefits & creation. URL : <https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture>.
2. How blockchain can impact the telecommunications industry and its relevance to the C-Suite // Deloitte. URL : [https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-mediatelecommunications/za\\_TMT\\_Blockchain\\_TelCo.pdf](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-mediatelecommunications/za_TMT_Blockchain_TelCo.pdf).
3. Блокчейн у телекомунікації: як Nexign та Bublestone модернізують галузь. URL : <https://nexign.com/en/blog/Blockchain-in-telecom>.
4. Блокчейн-Телеком или как технологии меняют правила игры. URL : <https://3commas.io/ru/blog/blokchejn-telekom-ili-kak-texnologii-menyayut-pravila-igry>.

### Manuilov Ya.S. USE OF BLOCKCHAIN TECHNOLOGY IN TELECOMMUNICATIONS

*The article considers the features of the technology blockchain, its advantages and disadvantages, the possibility of use in telecommunications systems, the provision of services by operators based on this technology. Transparency and flexibility of banking, financial and other types of transactions using blockchain technology. Maintaining public registers with a history that cannot be changed, conducting online voting, digital identity systems and notaries. Trust in systems based on blockchain technology is based on the clear implementation of all participants, a decentralized system established in the algorithms of the rules and verification of compliance with these rules by each participant. Even if an attacker tries to perform an erroneous, erroneous operation, each network member will automatically use software to verify the validity of the operation and reject it as erroneous. Failure of distributed telecommunications systems built using blockchain technology is considered. Use of smart contracts (smart contracts) in the provision of various types of telecommunications services. Principles of availability and immutability of information, transparency in transactions and maintenance of blockchain systems in telecommunications. The efficiency and expediency of using blockchain technology in telecommunication systems is analyzed. Possibilities of using this technology to optimize business processes in companies providing telecommunications services and in the banking sector are considered. The use of new virtual IDs of serviced subscribers, instead of obsolete ones, will simplify customer service, roaming agreements between operators and create opportunities for new types of services. The mathematical (cryptographic) basis of blockchain technology, based on hash functions and digital signature, which guarantees the integrity and immutability of information and the mechanism of verification of possession without the need to apply to an arbitrator, is considered. Opportunities and difficulties that may arise when implementing blockchain technology in existing telecommunications systems.*

**Key words:** blockchain, transactions, hash function, digital signature, decentralized networks, smart contracts, telecommunication services.