УДК 004.056.53:004.738.1
DOI: 10.31673/2409-7292.2024.010004

Замрій І. В., Шахматов І. О.

ПОТЕНЦІАЛ БЛОКЧЕЙНУ У ПОКРАЩЕННІ БЕЗПЕКИ ВЕБ-САЙТІВ

З цифровою трансформацією та зростанням кіберзагроз безпека веб-сайтів стала життєво важливою складовою розвитку Інтернету. Веб-сайти містять велику кількість конфіденційної інформації, такої як особисті дані користувачів, фінансова інформація та комерційні таємниці. Зловмисники постійно шукають вразливості для атак та крадіжок даних, що може призвести до серйозних наслідків для користувачів та власників веб-сайтів. У даному дослідженні проведено широкий аналіз та порівняльне дослідження ефективності технологій блокчейн у порівнянні з традиційними методами безпеки веб-сайтів. Основна увага дослідження зосереджена на оцінці ключових параметрів, таких як точність прийняття рішень, швидкість обробки запитів та загальна надійність системи. Під час дослідження виявлено вплив кількості блоків у ланцюжку блокчейну та якості шифрування на точність прийняття рішень. Проаналізовано здатність системи ефективно стримувати потенційні загрози. Швидкість обробки запитів оцінювалася з урахуванням можливого впливу збільшення кількості блоків і ускладнення шифрування на продуктивність системи. Розроблено комплексну формулу оцінки загальної надійності системи, яка поєднує позитивні та негативні аспекти технологій блокчейн. Отримані результати вказують, що інтегруючи фактори точності та швидкості обробки в комплексну оцінку надійності системи, використання блокчейну дозволяє підвищити загальну надійність системи захисту веб-сайтів.

Ключові слова: блокчейн, захист веб-сайтів, кібербезпека, технології розподіленого реєстру, шифрування даних, оптимізація продуктивності.

Вступ

З цифровою трансформацією та зростанням кіберзагроз безпека веб-сайтів стала життєво важливою складовою розвитку Інтернету. Веб-сайти містять велику кількість конфіденційної інформації, такої як особисті дані користувачів, фінансова інформація та комерційні таємниці. Зловмисники постійно шукають вразливості для атак та крадіжок даних, що може призвести до серйозних наслідків для користувачів та власників веб-сайтів. У цьому контексті важливо розглядати нові прогресивні технології, які можуть покращити безпеку веб-сайтів. Однією з таких технологій є блокчейн. Блокчейн – це децентралізована система, яка забезпечує безпеку даних шляхом розподіленого збереження інформації у вигляді блоків, які зв'язані криптографічною хеш-функцією. Це робить неможливим зміну чи вилучення даних без попереднього погодження всіма учасниками мережі.

Використання блокчейну для підвищення кібербезпеки веб-сайтів має ряд переваг, що можуть кардинально змінити спосіб захисту веб-сайтів завдяки децентралізованій структурі, незмінним записам і криптографічному шифруванню. Вона забезпечує високий рівень надійності та цілісності даних, оскільки будь-які спроби зміни інформації будуть виявлені та заблоковані. Блокчейн дозволяє зменшити ризик крадіжки даних, оскільки вони зберігаються у безпечному та недоступному для зловмисників форматі.

Це дослідження має на меті проаналізувати та порівняти ефективність блокчейн-технологій проти традиційних методів у контексті захисту веб-сайтів. Дослідження вивчає важливість прийняття рішень, швидкість обробки запитів і надійність системи в системах блокчейн, зосереджуючись на визначенні впливу кількості блоків і якості шифрування на ці параметри. Порівняння вказаних параметрів із параметрами традиційних систем безпеки дозволить оцінити потенційні переваги та недоліки.

Аналіз проблеми та літературних досліджень

Порівняно з централізованими базами даних, блокчейн є менш вразливим до кібератак завдяки своїй розподіленій природі. Хоча залишаються слабкі сторони, такі як ризики у керуванні мережею та атаки на цілісність. Вплив блокчейну на кібербезпеку залежить від зовнішніх факторів і контексту, в якому він реалізується, тому підвищення безпеки за допомогою блокчейну вимагає комплексного підходу, інтеграції з існуючими протоколами та усунення потенційних вразливостей на всіх технологічних рівнях [1, 2].

Технічні можливості та вразливі місця блокчейну є предметом постійного інтересу до того, як його можна використовувати в кібербезпеці [3]. Його ролі в наукових дослідженнях і

комерційному застосуванні приділяється значна увага. Вивчаючи ефективність блокчейну для захисту веб-сайтів, стає очевидним, що додавання блокчейну до стратегій кібербезпеки має важливе значення [4]. Результати роботи [5] підкріплюють дослідження того, як технологія блокчейну може підвищити безпеку веб-сайту порівняно зі звичайними методами, підкреслюючи важливість розробки комплексних заходів кібербезпеки, які враховують унікальні аспекти технології блокчейну.

Порівнюючи традиційну IT-безпеку з безпекою блокчейну, особливо в додатках і смарт-контрактах [6], ключові відмінності включають спільні елементи в традиційній розробці додатків і смарт-контрактів, особливості AppSec у блокчейні, технологічну зрілість, фрагментацію екосистеми, відкритість коду, відмінності в операційних середовищах і контролі доступу, різні підходи до безпеки, обмежені інструменти безпеки для розробників смарт-контрактів і різні регуляторні практики. Вказані відмінності підкреслюють унікальний характер безпеки блокчейну, який відрізняється від традиційних методів кібербезпеки.

Дослідження блокчейну та його аспектів безпеки розкривають ключові характеристики технології, такі як децентралізація, незмінність, можливість перевірки, прозорість і цілісність, простежуючи її розвиток з 1980-х років до створення Bitcoin та Ethereum. Алгоритми консенсусу, включаючи Proof of Work та Proof of Stake, відіграють ключову роль у підтримці блокчейну, а смарт-контракти, представлені Ethereum, революціонізують автоматизацію процесів [7].

У контексті зростання популярності Інтернет речей (IoT) важливість децентралізованого підходу управління довірою, який забезпечує блокчейн, стає ще більш важливим. Блокчейн використовується в різних сферах, забезпечуючи нові рівні прозорості та безпеки [8]. Цілі NIST щодо кібербезпеки демонструють, як блокчейн може відповідати сучасним вимогам безпеки, і підкреслюють необхідні обставини для його застосування. Систематичний огляд, що охоплює академічні та промислові дослідження, висвітлює різні підходи до кібербезпеки в системах, заснованих на блокчейні. Цей аналіз має вирішальне значення для проведення порівняльного дослідження ефективності блокчейну та традиційних методів захисту веб-сайтів, вказуючи на потенційні переваги та проблеми використання технології блокчейну для кібербезпеки.

Проведений аналіз безпеки блокчейн [9] розкриває його унікальні характеристики, такі як децентралізація, незмінність і прозорість, які роблять цю технологію цінною в різних галузях, а також відкривають нові шляхи для потенційних кібератак. Розглядаючи еволюцію блокчейну та його класифікацію на публічний, консорціумний і приватний типи, слід звернути увагу на різні рівні загроз безпеці та захисні методи, які можна застосувати. У контексті безпеки веб-сайтів важливо розуміти проблеми моніторингу мережі та традиційних централізованих систем управління, а також потенційне зловживання блокчейном. Враховуючи потенціал і складність технології блокчейн, застосування технології блокчейн не тільки створює загрози та виклики, але й відкриває можливості для покращення безпеки веб-сайтів [9]. Використання технології блокчейн для цілей кібербезпеки підкреслює її величезний потенціал для захисту зберігання та передачі даних через децентралізовану, надійну однорангову систему [10]. Особливо в таких сферах, як IoT, мережі, машинна візуалізація та безпечне зберігання персональних даних, блокчейн можна використовувати для підвищення безпеки. Зростання глобального інтересу до блокчейну в різних галузях, таких як логістика, фармацевтика та кібербезпека, демонструє його універсальність і значний вплив на кібербезпеку.

З моменту появи біткоїна у 2008 році розвиток технології блокчейн продемонстрував широту її застосування не лише у сфері криптовалют, а й у таких сферах, як охорона здоров'я, освіта та державне управління. Хоча основні концепції блокчейну, такі як децентралізація і незмінність, а також алгоритми консенсусу відіграють ключову роль у трансформації цифрових транзакцій і ведення діловодства, вони також висвітлюють проблеми, пов'язані з широкомасштабним впровадженням, включаючи технічні та екологічні аспекти [11].

© Замрій, І. В., & Шахматов, І. О. (2024). Потенціал Блокчейну у покращенні безпеки Веб-сайтів. Сучасний захист інформації, 1(57), 28–38. https://doi.org/10.31673/2409-7292.2024.010004.

Розуміння цих особливостей і викликів блокчейну має вирішальне значення для аналізу ефективності блокчейну в порівнянні з традиційними методами захисту веб-сайтів, а також для оцінки його потенціалу та обмежень в контексті кібербезпеки.

Інтеграція технології блокчейн у сферу кібербезпеки, особливо в освітньому секторі, відкриває нові можливості для посилення безпеки та автентичності систем перевірки кваліфікацій. В умовах стрімкого розвитку інтернет-технологій блокчейн пропонує альтернативний підхід до централізованої моделі перевірки, трансформуючи її в більш безпечну і децентралізовану форму і забезпечуючи надійне рішення проти видачі фальшивих дипломів [12]. Ця технологія відкриває нові шляхи для гарантування безпеки та автентичності цифрових сертифікатів і навчальних програм, а також для розширення їх використання в різних секторах. Проблеми управління різними пристроями IoT [13], що працюють на різних платформах і протоколах, вимагають розробки надійних механізмів безпеки, включаючи криптографічні ключі. Аналіз існуючих протоколів аутентифікації та управління ключами в IoT є важливим кроком у розвитку наступних технологій безпеки Застосування блокчейну і штучного інтелекту в IoT відкриває нові можливості для підвищення безпеки і висвітлює потенційні рішення для усунення вразливостей і атак [14].

Від біткоїна до його дедалі ширшого застосування в системах управління охороною здоров'я, блокчейн пропонує рішення для захисту медичних даних. У роботі [15] вивчаються ключові особливості блокчейну, такі як криптографія і смарт-контракти, які допомагають встановити довіру і безпеку, зокрема, виділено обмеження і проблеми в контексті конфіденційності пацієнтів і обміну даними. Тобто, специфічні проблеми безпеки на різних рівнях технології блокчейн вимагають постійних досліджень для вирішення поточних питань безпеки і вдосконалення її застосування в охороні здоров'я та інших секторах.

Поза початковою асоціацією з криптовалютами, технологія блокчейн у вищій освіті замінює традиційні академічні звіти новою моделлю обміну науковими знаннями та надання безпечних рішень, які докорінно змінюють академічні практики. Технологія підкреслює свою децентралізаційну та високозахищену природу, що важливо в контексті зростання кількості кіберзлочинів та витоків даних [16]. Незважаючи на такі проблеми, як вразливість до певних типів атак і високе енергоспоживання, блокчейн визнаний перспективним рішенням для управління даними в академічному середовищі.

Інтеграція технології блокчейн і транспортних мереж VANET відкриває нові можливості для підвищення безпеки та ефективності інтелектуальних транспортних систем [17]. VANET, які забезпечують базовий зв'язок між транспортними засобами та придорожніми пристроями, стикаються з проблемами, пов'язаними з динамічною топологією та високою мобільністю, що впливають на безпеку та конфіденційність. Блокчейн як децентралізована платформа пропонує вирішення цих проблем завдяки своїй прозорості, гнучкості та незмінності. Різні аспекти безпеки VANET, такі як децентралізований консенсус, мобільність і розподіл блоків, демонструють потенціал блокчейну для вирішення цих проблем і підкреслюють необхідність створення ефективної, масштабованої і безпечної системи.

Стрімке зростання кількості розумних пристроїв у мережах IoT призвело до значних викликів у сфері безпеки комунікацій, і інтеграція блокчейну є важливим рішенням, що дозволяє вирішити проблему обмежених ресурсів мережевих пристроїв та недоліків централізованих мереж: Багаторівнева архітектура на основі блокчейну для IoT спрощує впровадження і забезпечує безпеку, об'єднуючи різні рівні, які вимагають окремих стратегій безпеки. Кластеризація та багатошарові структури підвищують довговічність мережі, а архітектура системи безпеки реалізує надійні механізми захисту. Підхід кластеризації мережі використовує метаевристичні алгоритми оптимізації для підвищення продуктивності та масштабованості [18]. Такий підхід до застосування блокчейну в IoT важливий для покращення безпеки та управління даними, включаючи безпеку веб-сайтів, які можуть запропонувати аналогічні переваги в контексті кібербезпеки.

© Замрій, І. В., & Шахматов, І. О. (2024). Потенціал Блокчейну у покращенні безпеки Веб-сайтів. Сучасний захист інформації, 1(57), 28–38. https://doi.org/10.31673/2409-7292.2024.010004.

Технологія блокчейн призвела до значних змін у практиках кібербезпеки на підприємствах, запровадивши новий підхід до захисту цифрових активів. Дослідження вразливостей блокчейну та пов'язаних з ними загроз безпеці з використанням методів інтелектуального аналізу тексту та моделювання може допомогти виявити ключові тенденції та прогалини в цій сфері. Ключові питання дослідження [19] включають кореляцію між дослідженнями кібербезпеки та вразливостями блокчейну, типами кібератак на мережу та вплив на безпеку блокчейну.

Виклики та потенційні рішення для застосування технології блокчейн у сферах кібербезпеки та конфіденційності даних є важливими для розуміння її потенціалу. Особлива увага приділяється управлінню безпекою даних та дотриманню нормативної документації, таких як ISO 27001 та GDPR. З огляду на зростаючу залежність від хмарних обчислень і пристроїв IoT, надійні заходи кібербезпеки стають ще більш важливими. Малі та середні підприємства стикаються з унікальними проблемами в розумінні та впровадженні кібербезпеки, і завдяки блокчейну пропонується їх вирішення для забезпеченні цілісності даних в децентралізованому середовищі. [20].

Інтеграція технології блокчейн у кіберфізичні системи [2]. відкриває нові можливості для підвищення безпеки та ефективності, особливо в контексті збору даних IoT. Технологія блокчейн може допомогти вирішити проблеми, пов'язані з адаптацією блокчейну до кіберфізичних систем, підвищенням надійності та зменшенням вразливостей [21].

Інтеграція технології блокчейн у периферійні обчислення як спосіб забезпечення конфіденційності та безпеки даних є важливим аспектом сучасних досліджень. Однак з розвитком таких систем виникають певні проблеми з безпекою, особливо в контексті виявлення та відстеження вузлів у блокчейні, зокрема, нові підходи до виявлення таких вузлів використовують нейронні мережі в поєднанні зі стратегіями випадкових блукань для більш ефективного моніторингу [22].

Використання блокчейну для виявлення та зберігання мережевих топологій відкриває нові можливості для управління складними мережевими системами. Зі збільшенням кількості підключених пристроїв та урізноманітненням мережевих структур управління ними стає все більш складним і потребує розробки ефективних рішень. Розробка систем на основі блокчейну для безпечного виявлення та зберігання мережевих даних досліджено у роботі [23]. Такий підхід демонструє великий потенціал у порівнянні з традиційними методами управління мережею. Хоча блокчейн зазнав значних змін з моменту появи біткойна і його застосування в різних сферах зростає, він також стикається з уразливими місцями в безпеці, і для забезпечення безпеки на всіх рівнях архітектури потрібен комплексний підхід. Більшість досліджень зосереджені на конкретних темах, таких як безпека біткоїна або смарт-контрактів, але бракує досліджень, які надають всебічний огляд екосистеми блокчейну [24]. Систематичний аналіз блокчейн-сервісів з акцентом на безпеку, класифікацію вразливостей і механізми захисту на всіх рівнях, включаючи криптографію, консенсус і безпеку смарт-контрактів, міг би значно сприяти розвитку галузі, особливо в контексті безпеки веб-сайтів.

Мета дослідження

Метою цього дослідження є детальний аналіз і порівняння ефективності технології блокчейн і традиційних методів для безпеки веб-сайтів. Ключові аспекти, що розглядаються в цьому дослідженні, включають точність процесу прийняття рішень, швидкість обробки запитів і загальну надійність системи. Дослідження фокусується на тому, як кількість блоків у блокчейні та якість шифрування впливають на ці ключові показники і як ці фактори порівнюються з традиційними системами.

Точність рішень вимірюється відсотком успішно обійдених загроз від загальної кількості спроб доступу. Швидкість обробки визначається кількістю запитів, які можуть бути оброблені за одиницю часу. Загальна надійність системи поєднує ці два елементи, враховуючи, як збільшення кількості блоків і покращення шифрування впливає на загальну ефективність і безпеку системи, а також на потенційні втрати в швидкості обробки.

© Замрій, І. В., & Шахматов, І. О. (2024). Потенціал Блокчейну у покращенні безпеки Веб-сайтів. Сучасний захист інформації, 1(57), 28–38. https://doi.org/10.31673/2409-7292.2024.010004.

Метою цієї роботи є розуміння того, як блокчейн може підвищити безпеку і точність у захисті веб-сайтів порівняно з традиційними методами.

Математична модель та результати досліджень

Цифрові технології потребують забезпечення безпеки даних, особливо в умовах зростаючих кіберзагроз. У цьому відношенні технологія блокчейн виділяється як інноваційне рішення для підвищення безпеки в порівнянні з традиційними методами. Важливим аспектом є оцінка ефективності блокчейн-систем у запобіганні загрозам безпеки порівняно з традиційними системами.

Для того, щоб оцінити ефективність технології блокчейн у порівнянні з традиційними системами, пропонується застосувати математичну модель, засновану на логістичних функціях. Ця модель дозволяє проаналізувати, як збільшення кількості блоків у блокчейні впливає на точність системи у запобіганні та протидії загрозам безпеці.

Точність блокчейн-системи оцінюється за формулою (1)

$$A_{BC} = A_{base} + \frac{L}{1+e^{-k(B-x_0)}}, \tag{1}$$

де A_{BC} – точність блокчейн-системи,

A_{base} – базова точність системи, яка в даному дослідженні встановлюється на рівні 80%,

L – максимальне збільшення точності, яке встановлено на рівні 20%,

B – кількість блоків у блокчейн-системі,

k – коефіцієнт приросту, який характеризує швидкість зростання функції,

x_0 – точка, у якій функція починає стрімко зростати.

Для традиційної системи точність вважається сталою величиною і не залежить від кількості блоків чи інших зовнішніх факторів (2), тому

$$A_T = A_{base}, \tag{2}$$

де A_T є точністю традиційної системи.

Щоб проілюструвати цю модель, в таблиці (Табл. 1) показано, як точність системи блокчейн покращується з кожним наступним блоком. Таблиця чітко показує поступове збільшення точності, починаючи з базової точності для одного блоку. Однак важливо відзначити, що цей темп зростання ніколи не перевищує 100%, що відповідає реалістичній моделі підвищення точності блокчейну. У той же час точність традиційної системи стабільно тримається на рівні 80%.

Таблиця 1

Порівняння точності блокчейн-системи в залежності від кількості блоків

Кількість блоків	Точність блокчейну (Модифікована Логістична)	Точність традиційної системи
1	0.819	0.80
2	0.824	0.80
3	0.830	0.80
4	0.836	0.80
5	0.845	0.80
6	0.854	0.80
7	0.864	0.80
8	0.876	0.80
9	0.888	0.80
10	0.900	0.80

Для наочності та більш детального аналізу візуалізації цих результатів використовується графік (Рисунок 1). На графіку чітко видно, що точність блокчейн-системи зростає з кожним новим блоком, тоді як точність традиційної системи залишається незмінною. Це відображає важливу перевагу технології блокчейн в контексті безпеки, а саме її здатність підвищувати ефективність в міру розширення мережі.

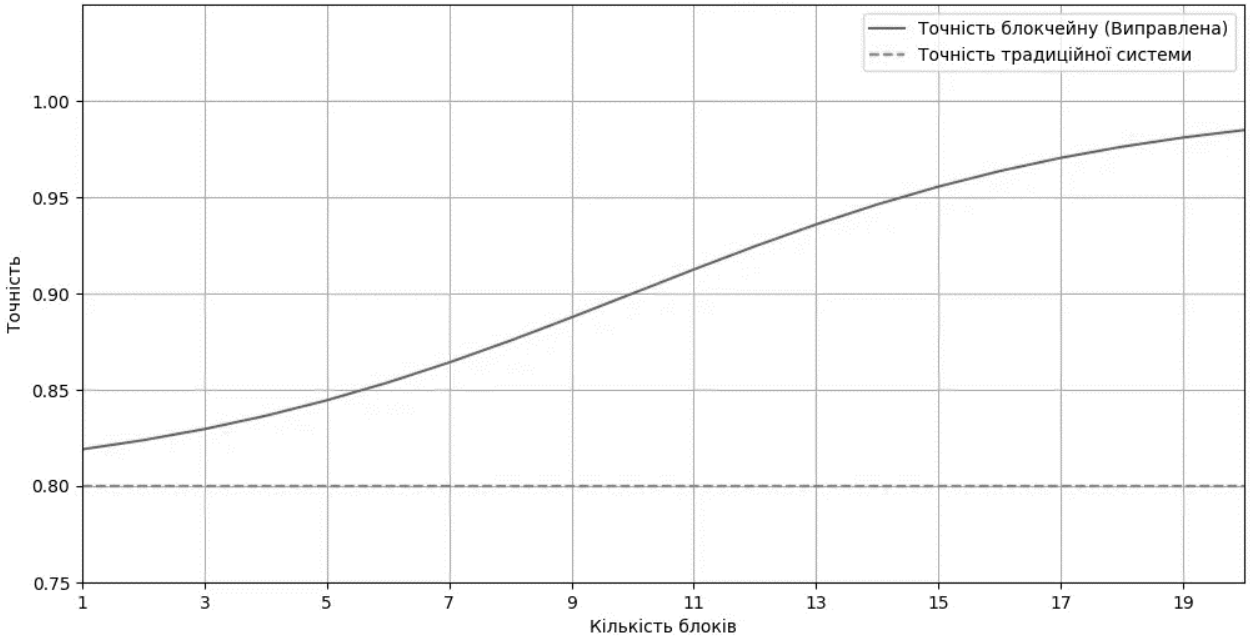

Рис. 1. Порівняння точності традиційної системи та блокчейну в залежності від кількості блоків

Цей метод порівняння показує, що блокчейн стає більш ефективним у захисті даних зі збільшенням кількості блоків. Це підкреслює потенційні переваги блокчейну в тих сферах, де важлива надійність і безпека даних.

Однак важливо зазначити, що впровадження технології блокчейн може мати й інші наслідки, зокрема, з точки зору швидкості обробки заяв на виплату страхових відшкодувань. Хоча блокчейн підвищує безпеку, він також може вплинути на ефективність системи в цілому, особливо при обробці великої кількості заяв. Тому, щоб повністю зрозуміти вплив технології блокчейн, необхідно також розглянути, як вона може вплинути на швидкість обробки даних.

Якщо використовувати залежність швидкості обробки від кількості блоків для порівняння змін у швидкості обробки запитів у системі блокчейн, то швидкість обробки зменшується зі збільшенням кількості блоків. Це відображає той факт, що зі збільшенням ланцюжка блоків у блокчейні збільшується час, необхідний для обробки транзакцій і запитів. Запропонована математична модель для такого порівняння виражається рівністю:

$$S_{BC} = \frac{S_{base}}{1 + a \times (\mathrm{B} - 1)}, \tag{3}$$

де S_{BC} – швидкість обробки запитів блокчейн-системою,

S_{base} – базова швидкість обробки запитів,

B – кількість блоків в блокчейні,

a – коефіцієнт, що кількісно характеризує як збільшення кількості блоків впливає на зниження швидкості обробки.

© Замрій, І. В., & Шахматов, І. О. (2024). Потенціал Блокчейну у покращенні безпеки Веб-сайтів. Сучасний захист інформації, 1(57), 28–38. https://doi.org/10.31673/2409-7292.2024.010004.

У даній моделі за наявності одного блоку швидкість обробки визначається як базова (S_{base}), але з кожним новим блоком швидкість обробки знижується. А за допомогою коефіцієта (a) можна регулювати інтенсивність цього зниження.

З іншого боку швидкість обробки запитів для традиційної системи залишається незмінною і може бути описана як стала величина (4):

$$S_T = S_{base}. \tag{4}$$

Таким чином, модель дозволяє порівняти, як змінюється швидкість обробки заяв в блокчейн-системі в залежності від кількості блоків у порівнянні з сталою швидкістю традиційної системи.

Для того, щоб проаналізувати дані про швидкість обробки заяв в блокчейн-системі в залежності від кількості блоків, припускається, що базова швидкість обробки традиційної системи становить 100 заяв на секунду і це число залишається незмінним за будь-яких умов. З іншого боку, ця швидкість зменшується зі збільшенням кількості блоків у блокчейн-системі, оскільки кожен додатковий блок обробляється довше. Результати розрахунків наведені в таблиці (Табл. 2).

Таблиця 2

Порівняння швидкості обробки запитів блокчейн-системи в залежності від кількості блоків

Кількість блоків	Швидкість блокчейну (запитів/сек)	Швидкість традиційної системи (запитів/сек)
1	100.00	100
2	95.24	100
3	90.91	100
4	86.96	100
5	83.33	100
6	80.00	100
7	76.92	100
8	74.07	100
9	71.43	100
10	68.97	100

Візуальне представлення даних на графіку (Рис. 2) ілюструє, як швидкість обробки запитів у блокчейн-системі зменшується з кожним новим блоком. У порівнянні зі сталою швидкістю традиційної системи, очевидний потенційний компроміс між безпекою та ефективністю, який виникає при використанні блокчейн-технологій.

Порівняння цих двох підходів показує, що блокчейн може забезпечити більшу безпеку і надійність, ніж традиційні системи, але швидкість транзакцій і запитів може бути нижчою. Цей факт слід враховувати при виборі технології для конкретного застосування, де швидкість обробки даних є важливим фактором.

Для того, щоб оцінити надійність систем, заснованих на блокчейні, запропоновано математичну модель, яка враховує кількість блоків у ланцюжку. Основна гіпотеза цієї моделі полягає в тому, що надійність системи зростає зі збільшенням кількості блоків. Це відображає характеристики блокчейну, де безпека зростає з кожним новим блоком, що ускладнює несанкціоноване втручання.

Пропонується визначати надійність технології блокчейн для безпеки додатків за допомогою модифікованої логістичної функції:

$$R_{BC} = R_{base} + \frac{L_R}{1 + e^{-k_R(B - x_{0R})}}, \tag{5}$$

де R_{BC} – надійність блокчейн-системи,

R_{base} – базова надійність системи, що набуває однакових значень для традиційної системи та блокчейн-системи з одним блоком,

L_R – параметр, що характеризує максимальне збільшення надійності від базової величини,

k_R – коефіцієнт приросту, що характеризує швидкість наближення до максимальної надійності,

x_{0R} – точка стрімкого зростання надійністі,

B – кількість блоків в блокчейн-системі.

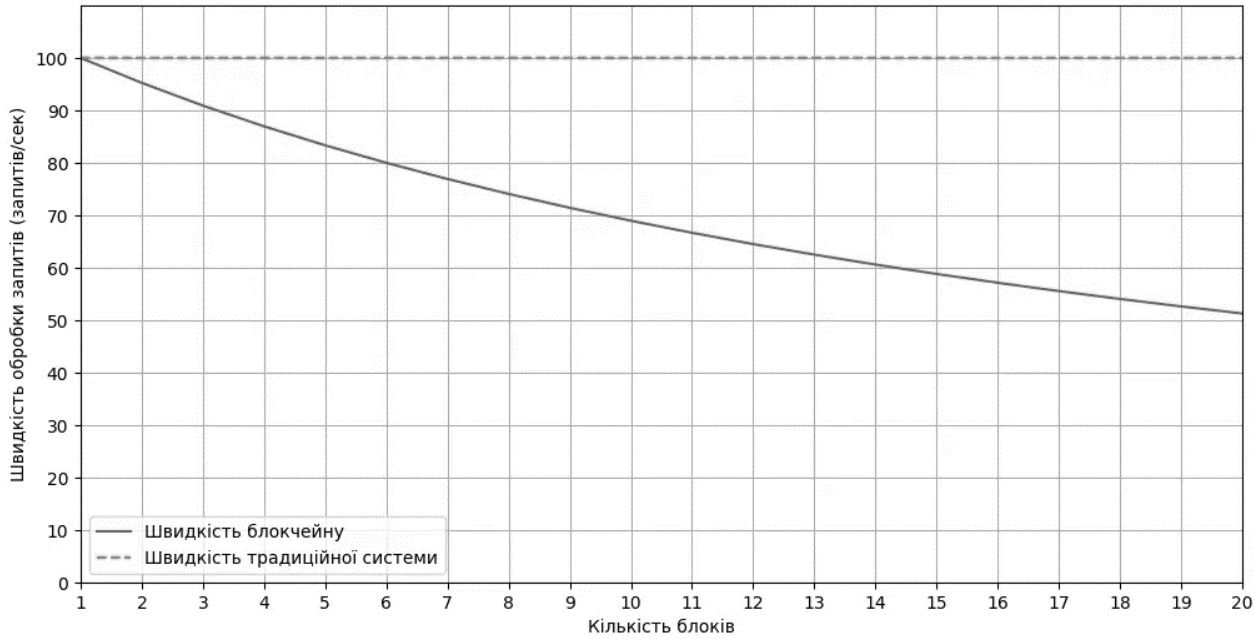

Рис. 2. Швидкість обробки запитів блокчейн-системи в порівнянні з традиційною системою

Надійність традиційної системи (R_{T}) моделюється як стала величина, незалежна від кількості блоків:

$$R_T = R_{base}, \tag{6}$$

Це відображає характеристики традиційних систем, де надійність не змінюється з часом або зі зміною внутрішніх параметрів системи. Застосовуючи цю модель, можна спрогнозувати, як збільшення кількості блоків у блокчейні впливає на надійність системи порівняно з традиційною системою. Модель підкреслює одну з головних переваг блокчейну – його здатність забезпечувати вищу надійність і безпеку зі збільшенням розміру мережі. Результати, отримані за допомогою цієї моделі, представлені в таблиці (Табл. 3).

Для більш наочного уявлення про вплив кількості блоків на надійність системи, дані візуалізовано графіку (Рис. 3). Графік демонструє як зі збільшенням кількості блоків надійність блокчейн-системи поступово зростає.

Порівнюючи надійність блокчейн і традиційних систем, можна побачити, що блокчейн має значну перевагу, особливо з точки зору захисту даних і запобігання кібератакам. З точки зору безпеки, збільшення кількості блоків у блокчейні є важливим фактором підвищення загальної надійності системи. Це підкреслює потенціал використання блокчейну в різних сферах, де важлива надійність.

Були розглянуті різні аспекти моделювання та аналізу технології блокчейн у порівнянні з традиційними системами. Основна увага була зосереджена на оцінці точності, швидкості обробки запитів і надійності обох систем залежно від кількості блоків у блокчейні.

Таблиця 3

Порівняння надійності блокчейн-системи в залежності від кількості блоків

Кількість блоків	Надійність блокчейну	Надійність традиційної системи
1	0.854	0.800
2	0.864	0.800
3	0.876	0.800
4	0.888	0.800
5	0.900	0.800
6	0.912	0.800
7	0.924	0.800
8	0.936	0.800
9	0.946	0.800
10	0.955	0.800

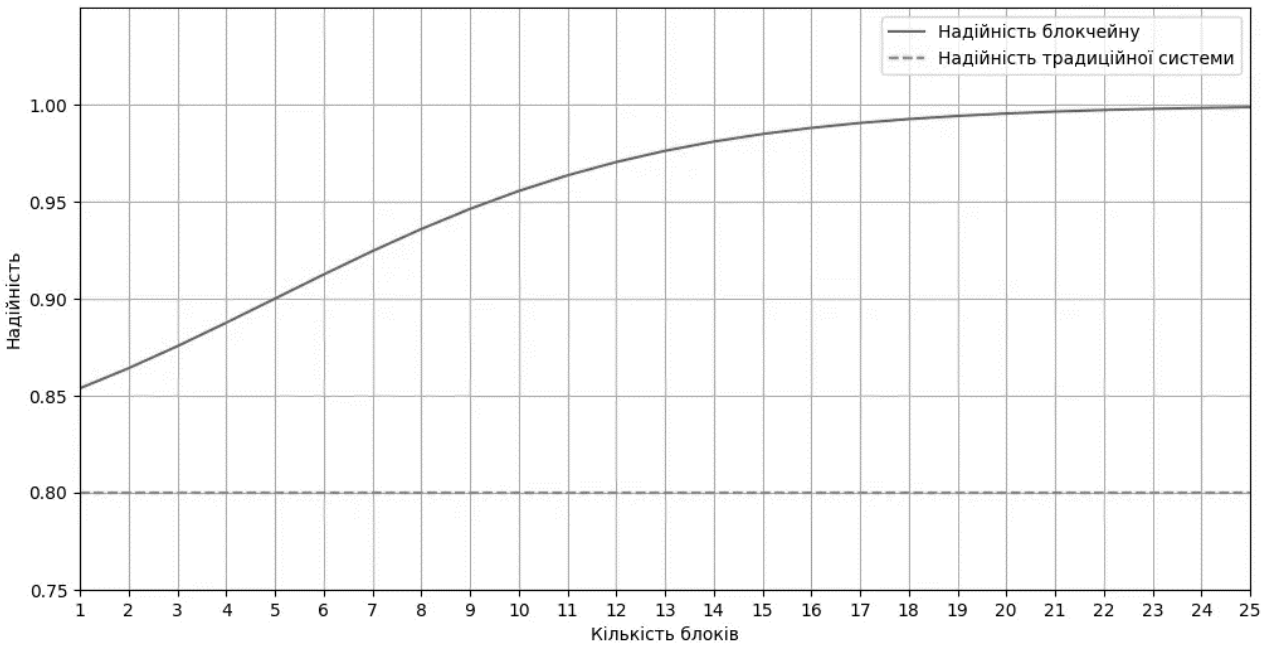

Рис. 3. Надійність блокчейн в порівнянні з традиційною системою

© Замрій, І. В., & Шахматов, І. О. (2024). Потенціал Блокчейну у покращенні безпеки Веб-сайтів. Сучасний захист інформації, 1(57), 28–38. https://doi.org/10.31673/2409-7292.2024.010004.

Для кількісної оцінки того, як збільшення кількості блоків у блокчейні впливає на ці ключові показники, було використано математичну модель. Результати показали, що зі збільшенням кількості блоків точність роботи блокчейн-системи поступово зростає, тоді як швидкість обробки запитів знижується. Надійність блокчейн також зростає з кожним новим блоком, забезпечуючи перевагу в безпеці та надійності над традиційними системами.

Ці результати допомагають краще зрозуміти потенційні переваги та недоліки блокчейну. З одного боку, блокчейн підвищує безпеку і надійність, які важливі для веб-сайту. З іншого боку, він може впливати на швидкість обробки даних, що є важливим фактором для систем, де швидкість є ключовою вимогою. Тому вибір між технологією блокчейн і традиційними системами повинен ґрунтуватися на зваженому аналізі вимог конкретного застосування і важливості різних показників, таких як безпека, швидкість і надійність. Розроблена модель та методологія дослідження надають інструменти для такого аналізу та дозволяють застосовувати кількісні методи для оцінки потенційних переваг та обмежень блокчейну порівняно з традиційними підходами.

Висновки

У дослідженні представлено комплексний аналіз та порівняння технології блокчейн з традиційними методами у сфері безпеки веб-сайтів, а також визначено важливі аспекти та відмінності між цими підходами. Аналіз показав, що технологія блокчейн значно підвищує точність процесу прийняття рішень. Це пов'язано, зокрема, з її здатністю ефективно запобігати загрозам, що досягається за рахунок збільшення кількості блоків і поліпшення шифрування, що є перевагою в порівнянні з традиційними системами. З іншого боку, також було відзначено, що збільшення кількості блоків і підвищення складності шифрування в системах блокчейн може призвести до зниження швидкості обробки даних. Цей висновок вказує на потенційний компроміс між безпекою та продуктивністю системи, що є важливим фактором при впровадженні блокчейн-систем.

Інтеграція факторів точності та швидкості обробки в комплексну оцінку надійності системи показує, що використання блокчейну може значно підвищити загальну надійність систем безпеки веб-сайтів.

В цілому, ці дослідження показують великий потенціал технології блокчейн у сфері безпеки веб-сайтів, але також підкреслюють важливість пошуку балансу між різними аспектами безпеки та продуктивності.

Дослідження вказують на важливі напрямки для майбутніх досліджень технології блокчейн та її застосування в кібербезпеці. Одним з важливих аспектів є розробка методів оптимізації блокчейн-систем, що передбачають пошук шляхів мінімізації впливу на швидкість обробки запитів при збереженні високого рівня безпеки і точності.

Перелік посилань

1. How Effective Is Blockchain in Cybersecurity? [Електронний ресурс] // ISACA Journal. Режим доступу: www.isaca.org/resources/isaca-journal/issues/2021/volume-4/how-effective-is-blockchain-in-cybersecurity.

2. Sobchuk, V., Zamrii, I., Laptiev, S. Ensuring Functional Stability of Technological Processes as Cyberphysical Systems Using Neural Networks // Lecture Notes in Networks and Systems, 2023, Volume 536, pp. 581–592.

3. Liu, M., Yeoh, W., Jiang, F., Choo, K.-K. R. Blockchain for Cybersecurity: Systematic Literature Review and Classification // Journal of Computer Information Systems, 2021, pp. 1182-1198.

4.Шахматов, І.О., Замрій, І.В. Технологія blockchain як інструмент протидії неправомірному використанню доступу до веб-сайтів // Міжнародна науково-практична конференція молодих вчених та студентів «Інженерія програмного забезпечення і передові інформаційні технології» (SoftTech-2023), присвячена 125-тій річниці КПІ імені І.Сікорського, 19-21 грудня 2023 року, Київ, Україна, с. 360-364.

5. Mahmood, S., Chadhar, M., Firmin, S. Cybersecurity Challenges in Blockchain Technology: A Scoping Review // Human Behavior and Emerging Technologies, 2022, Volume 2022, Article ID 7384000, 11 p.

6. How Blockchain Security Differs From Traditional Cybersecurity [Електронний ресурс] // Crypto & Blockchain Security, 2022. Режим доступу: https://cryptosec.com/crypto-blockchain-security/smart-contracts-security/.

7. Guo, H., Yu, X. A survey on blockchain technology and its security // Blockchain: Research and Applications, 2022, Volume 3, Issue 2, June 2022, 100067.

© Замрій, І. В., & Шахматов, І. О. (2024). Потенціал Блокчейну у покращенні безпеки Веб-сайтів. Сучасний захист інформації, 1(57), 28–38. https://doi.org/10.31673/2409-7292.2024.010004.

8. Gimenez-Aguilar, M., de Fuentes, J. M., Gonzalez-Manzano, L., Arroyo, D. Achieving cybersecurity in blockchain-based systems: A survey // Future Generation Computer Systems, 2021, Volume 124, pp. 91-118.

9. Wang, H., Wang, Y., Cao, Z., Li, Zh., Xiong, G. An Overview of Blockchain Security Analysis // China Cyber Security Annual Conference, 2019, CNCERT 2018: Cyber Security, pp. 55–72.

10. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., Choo, K.-K. R. A systematic literature review of blockchain cyber security // Digital Communications and Networks, 2020, Volume 6, Issue 2, pp. 147-156.

11. Tripathi, G., Ahad, M. A., Casalino, G. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges // Decision Analytics Journal, 2023, Volume 9, 100344.

12. Maulani, G., Gunawan, G., Leli, L., Ayu Nabila, E., Yestina Sari, W. Digital Certificate Authority with Blockchain Cybersecurity in Education // International Journal of Cyber and IT Service Management, 2021, 1(1), pp. 136–150.

13. Макарцев, М. О., Тушич, А. М., Замрій, І. В., Алексіна, Л. Т. Проблеми, труднощі та можливості IoT та хмарних обчислень // Зв'язок, 2021, №4. – С. 20-25.

14. Attkan, A., Ranga, V. Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security // Complex & Intelligent Systems, 2022, Volume 8, pp. 3559–3591.

15. Wenhua, Zh., Qamar, F., Abdali Taj-Aldeen, N., Hassan, R., Jafri, S. T. A., Nguyen, Q. N. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends // Electronics, 2023, 12(3), 546.

16. Mulyati, M., Ilamsyah, I., Ari,s A., Gunawan, I., Suzaki Zahran, M. Blockchain Technology: Can Data Security Change Higher Education Much Better? // International Journal of Cyber and IT Service Management, 2021, 1(1), pp. 121–135.

17. Grover, J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review // Vehicular Communications, 2022, Volume 34, 100458.

18. Honar, P. H., Rashid, M., Alam, F., Demidenko, S. Multi-Layer Blockchain-Based Security Architecture for Internet of Things // Sensors, 2021, 21(3), 772.

19. Prakash, R., Anoop, V. S., Asharaf ,S. Blockchain technology for cybersecurity: A text mining literature analysis // International Journal of Information Management Data Insights, 2022. Volume 2, Issue 2, 100112.

20. Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jaya,l A., Khan, I., Hewage, Ch., Platts J. Cybersecurity, Data Privacy and Blockchain: A Review // Computer Science, 2022, Volume 3, article number 127.

21. Khalil, A. A., Franco, J., Parvez, I., Uluagac, S., Shahriar, H., Rahman, M. A. A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems // 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), 2022, pp. 1774-1779.

22. Wang, Sh., Liu, Zh., Wang, H., Wang, J. Ensuring security in edge computing through effective blockchain node detection // Journal of Cloud Computing, 2023, volume 12, Article number 88.

23. Prashar, D., Jha, N., Shafi, M., Ahmad, N., Rashid, M., Banday, Sh. A., Khan, H. U. Blockchain-Based Automated System for Identification and Storage of Networks // Security and Communication Networks, 2021, Volume 2021, Article ID 6694281.

24. Chen, H., Luo, X., Shi, L., Cao, Y., Zhang, Y. Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective // Blockchain: Research and Applications, 2023, Volume 4, Issue 3, 100135.

Надійшла 08.01.2024