КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.5068
УДК 004.056.5

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

Петрів Петро Петрович
аспірант кафедри «Захист інформації»
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0000-7426-3696
petro.p.petriv@lpnu.ua

ЕФЕКТИВНІСТЬ БЛОКЧЕЙН-ЛОГУВАННЯ І SSO В МЕХАНІЗМАХ КІБЕРБЕЗПЕКИ

Анотація. Зі зростанням кіберзагроз в епоху цифрової трансформації, захист інформаційних систем стає вирішальним для забезпечення надійності та безпеки даних. Особливо це стосується систем автентифікації та логування, які є ключовими елементами в ідентифікації та протидії несанкціонованому доступу. Використання однакових облікових даних та традиційних методів аутентифікації відкриває широкі можливості для кіберзлочинців. У даній статті досліджується використання технології блокчейн як засобу боротьби з кіберзагрозами через впровадження незмінних, децентралізованих систем логування та аутентифікації. Блокчейн надає унікальні переваги, такі як незмінність даних та розподілене зберігання, що може значно ускладнити несанкціоноване втручання в системи безпеки. Розглядаються актуальні тенденції у сфері кібербезпеки, зокрема виклики, пов'язані з компрометацією даних та неефективним обміном інформацією між системами. Важливою частиною статті є аналіз останніх досліджень, зосереджений на можливостях блокчейну у розвитку систем ідентифікації та автентифікації, що базуються на децентралізованих ідентифікаторах та інтеграції технологій консенсусу. Основна мета дослідження — виявити та розробити технологічні рішення, спрямовані на підвищення безпеки, стійкості та ефективності систем логування та аутентифікації через застосування блокчейну. Додатково розглядаються інноваційні підходи в ідентифікації та аутентифікації, які можуть зміцнити захист від кіберзагроз.

Ключові слова: блокчейн; кібербезпека; автентифікація; логування; децентралізовані ідентифікатори; технології консенсусу; NFT; кіберзагрози.

ВСТУП

Розвиток технологій у останні десятиліття значно розширив можливості інтернету, сприяючи збільшенню цифрового взаємодії між користувачами. Системи одного входу (SSO) відіграють ключову роль у спрощенні доступу та підвищенні безпеки автентифікації, але зі зростанням кількості цифрових послуг виникає потреба у більш комплексних рішеннях для управління доступом та захисту інформації.

Блокчейн, зі своїми принципами децентралізації та безпеки, пропонує новітні можливості для вирішення цих викликів, зокрема в контексті систем SSO, відкриваючи шлях до ефективнішої та безпечнішої цифрової взаємодії. Розглядаючи концепцію застосування блокчейн у контексті технології SSO, ми відкриваємо перед собою широкий горизонт можливостей, що поєднують безпеку, децентралізацію та зручність для користувача.

У цій статті ми дослідимо, як блокчейн може підвищити рівень безпеки автентифікації, забезпечити децентралізований контроль доступу, зберігати дані користувачів та вирішувати інші аспекти, що стосуються системи SSO. Розглянемо вплив цієї технологічної симбіозу на сферу безпеки інтернет-взаємодії та роль, яку він може відіграти у подальшому розвитку цифрового світу.

Поглиблюючи наше розуміння взаємодії між блокчейн і SSO, ми виявимо, як ця інтеграція може визначати нові стандарти для безпеки та ефективності в сучасному цифровому ландшафті.

Постановка проблеми. Традиційні системи логування та автентифікації часто виявляються недостатньо ефективними перед обличчям розширеного спектру кібератак. Виклики, пов’язані зі збереженням цілісності та конфіденційності користувацьких даних, вимагають нових технологічних рішень. Блокчейн, із своїми принципами децентралізації, незмінності та прозорості, пропонує перспективні можливості для зміцнення кібербезпеки, але його інтеграція в існуючі системи автентифікації та логування викликає нові питання та виклики.

Актуальні аспекти проблеми:

1. Зростання кіберзагроз: Кіберзлочинці постійно вдосконалюють свої методи атак, використовуючи вразливості у традиційних системах безпеки, що підвищує ризик несанкціонованого доступу та витоку даних.
2. Централізація як слабкість: Централізоване зберігання даних створює єдині точки відмови, що спрощує завдання зловмисників при організації атак на системи.
3. Проблеми з обміном та зберіганням даних: Недоліки в системах управління та обміну даними можуть призвести до втрати цінної інформації та ускладнюють процеси аутентифікації та верифікації.

Враховуючи вищезазначені виклики, стає очевидною актуальність пошуку та впровадження інноваційних технологічних рішень, здатних протистояти кіберзагрозам на новому рівні. Блокчейн, зі своїми унікальними характеристиками, пропонує перспективний підхід до реформування систем логування та автентифікації, забезпечуючи вищий рівень безпеки, децентралізацію управління даними, та підвищену надійність цих систем у цифровому світі. Ця технологія відкриває нові горизонти у забезпеченні цілісності та конфіденційності даних, роблячи процеси логування та автентифікації більш прозорими та відповідними до вимог сучасної кібербезпеки.

Аналіз останніх досліджень і публікацій. В останні роки блокчейн став одним із ключових інструментів у стратегіях кібербезпеки, пропонуючи новітні підходи до забезпечення безпеки логування та автентифікації. Завдяки своїй децентралізованій структурі та незмінності записів, блокчейн забезпечує виняткові можливості для захисту від кіберзагроз, покращення цілісності даних та забезпечення прозорості операцій.

Децентралізація як захист від маніпуляцій: Блокчейн знижує ризик маніпуляцій з даними та несанкціонованого доступу через свою децентралізовану природу, розподіляючи записи по мережі вузлів. Це гарантує, що навіть у разі атаки на один вузол, інші елементи мережі залишаються недоторканими, забезпечуючи високий рівень безпеки інформації [1].

Логування та аудит: Блокчейн пропонує надійну систему логування та аудиту, де кожна транзакція незмінно записується і може бути перевірена. Це не тільки сприяє виявленню спроб несанкціонованого доступу чи інших безпекових інцидентів, але й забезпечує засоби для їх розслідування та відновлення [2].

Автентифікація та ідентифікація: Використання блокчейну для цифрових ідентифікаторів та автентифікації дозволяє створити системи з високим рівнем довіри та мінімальним ризиком фальсифікації чи крадіжки ідентифікаційних даних. Механізми, такі як докази з нульовим знанням, дозволяють автентифікувати користувачів без необхідності розкривати конфіденційну інформацію [3].

Виклики та перспективи: Незважаючи на значні переваги, впровадження блокчейну у сфері кібербезпеки супроводжується викликами, включаючи потребу в складних механізмах консенсусу, масштабування та управління ключами. Проте, постійний розвиток технології обіцяє нові рішення для цих проблем, роблячи блокчейн незамінним інструментом у боротьбі з кіберзагрозами.

Мета статті. Основною метою цієї статті є є аналіз ефективності використання блокчейн-технологій для логування та систем SSO у контексті кібербезпеки. Зокрема як саме ці технології можуть сприяти підвищенню захищеності цифрових систем і даних від несанкціонованого доступу, забезпечуючи при цьому високий рівень прозорості та надійності процесів автентифікації та авторизації. Окрема увага буде приділена аналізу переваг і недоліків інтеграції цих технологій, визначенню потенційних викликів, а також розробці рекомендацій для їх подолання та оптимізації використання в майбутньому.Основними завданнями статті є:

- Глибокий огляд блокчейн технології: дослідження основних принципів та переваг блокчейну, особливо з акцентом на забезпечення безпеки, надійності та прозорості в процесах логування та автентифікації.
- Аналіз поточного стану систем автентифікації: розгляд переваг та недоліків існуючих методів автентифікації з точки зору кібербезпеки, ідентифікація основних викликів та проблем, які можуть бути вирішені за допомогою блокчейну.
- Виявлення проблем у сфері кібербезпеки: ідентифікація та аналіз ключових проблем, пов’язаних з кіберзагрозами, що впливають на системи автентифікації та логування, та розгляд можливостей блокчейну для їх подолання.
- Визначення ролі блокчейну у захисті від кіберзагроз: оцінка потенціалу використання блокчейну для підвищення безпеки автентифікації та логування, а також подолання існуючих безпекових викликів.
- Розробка концепції використання блокчейну: пропозиція концептуального підходу до використання блокчейну для покращення процесів логування та автентифікації, з урахуванням технічних та функціональних аспектів.

Покращення систем аутентифікації через блокчейн

У сучасному світі, де кіберзагрози стають все більш різноманітними та складними, блокчейн пропонує революційні підходи до забезпечення безпеки систем аутентифікації. Одним з ключових напрямків використання блокчейну є розробка безпечних механізмів аутентифікації, здатних протистояти сучасним кіберзагрозам. Це особливо актуально у контексті розширення технологій Інтернету речей (IoT) та обчислень у тумані (fog computing), де зростання кількості з’єднаних пристроїв веде до підвищення ризиків безпеки. Використання блокчейну, зокрема на платформі Ethereum для реалізації механізмів аутентифікації через програмовані смарт-контракти, стає популярним рішенням завдяки його безпеці та швидкодії. [4].

Дослідження, присвячене використанню блокчейну для покращення продуктивності аутентифікаційних механізмів у середовищах fog computing, демонструє значний потенціал цієї технології. Пропонований механізм аутентифікації на основі Neo blockchain виявився значно швидшим за існуючі методи, зменшуючи час виконання процесів реєстрації та аутентифікації. Це відкриває нові перспективи для розробки більш ефективних та безпечних систем аутентифікації, що можуть задовольнити вимоги сучасних інформаційних систем [2].

На додаток, інше дослідження розкриває можливості блокчейну у створенні систем аутентифікації на основі моделі нульового довір'я (zero-trust). Ці системи вимагають верифікації аутентичності перед кожним доступом до мережі або ресурсу, забезпечуючи високий рівень безпеки від внутрішніх та зовнішніх загроз. Реалізація таких систем на базі блокчейну може значно підвищити захищеність цифрових ідентифікаторів і даних, мінімізуючи ризики витоку інформації [5].

Застосування блокчейну в аутентифікаційних системах не обмежується лише покращенням безпеки. Ця технологія також пропонує новітні методи зменшення обсягу переданих даних під час процесу аутентифікації, що є критично важливим для залізничних комунікаційних мереж та інших критичних інфраструктур. Зокрема, блокчейн може допомогти в реалізації ефективних схем аутентифікації, зменшуючи навантаження на мережу та підвищуючи загальну продуктивність системи. Це особливо важливо у сценаріях, де велика кількість пристроїв постійно перевіряє свою аутентичність, наприклад, у середовищах IoT [5].

Крім технічних переваг, інтеграція блокчейну у системи аутентифікації також сприяє підвищенню довіри та відкритості між учасниками. Завдяки децентралізованому зберіганню даних та незмінності записів, блокчейн забезпечує високий рівень прозорості та можливість перевірки будь-якої транзакції чи аутентифікаційного запиту. Це важливо не тільки для забезпечення безпеки, але й для створення системи, в якій користувачі та організації можуть взаємодіяти без страху перед маніпуляціями чи шахрайством.

Проте, попри численні переваги, впровадження блокчейну в аутентифікаційні системи супроводжується певними викликами. Однією з основних проблем є потреба у розробці нових стандартів та протоколів, що дозволяє інтегрувати цю технологію у вже існуючі IT-інфраструктури без збоїв у роботі та з мінімальними затратами. Також, питання масштабування блокчейн-мереж та забезпечення їх здатності обробляти великі обсяги аутентифікаційних запитів в реальному часі потребують додаткових досліджень та технологічних розробок.

Незважаючи на ці виклики, потенціал блокчейну у сфері аутентифікації залишається величезним. Постійний розвиток технології та поява нових рішень можуть значно підвищити ефективність, безпеку та надійність систем аутентифікації. В результаті, блокчейн має всі шанси стати ключовим елементом в архітектурі майбутніх безпечних цифрових середовищ. Аналіз переваг та недоліків наведено у табл. 1.

Таблиця 1

Аналіз переваг та недоліків

Переваги	Недоліки
Надійність та незмінність даних. Блокчейн забезпечує високий рівень безпеки через криптографічне хешування та децентралізацію, що робить майже неможливим несанкціоноване змінення логів.	Складність інтеграції. Інтеграція блокчейн-технологій у існуючі IT-інфраструктури може бути складною та вимагати значних витрат часу та ресурсів.
Прозорість та аудитабельність. Логи, збережені в блокчейні, легко перевіряються та доступні для аудиту, забезпечуючи високий рівень прозорості дій системи.	Масштабування. Блокчейн може зіткнутися з проблемами масштабування, особливо у публічних блокчейнах, де висока кількість транзакцій може сповільнити обробку.
Зниження ризику втрати даних. Розподілений характер блокчейну забезпечує додатковий рівень відмовостійкості та знижує ризик втрати даних через атаки або збої.	Вартість. Розгортання та підтримка блокчейн-рішень може бути коштовною, особливо з урахуванням необхідності спеціалізованих розробників та апаратного забезпечення.
Покращення механізмів автентифікації та авторизації. Інтеграція SSO дозволяє користувачам безпечно та ефективно управляти своїми цифровими ідентифікаторами, спрощуючи процес входу в системи без зниження рівня безпеки.	Залежність від провайдерів SSO. Використання SSO може створити залежність від конкретних провайдерів або технологій, обмежуючи гнучкість вибору рішень у майбутньому.
Блокчейн може бути адаптований до різних потреб і масштабів використання, від невеликих до великих систем.	Для деяких блокчейн-платформ, особливо для тих, що використовують доказ роботи (Proof of Work), масштабування може стати проблемою через високі енергетичні вимоги та обмеження швидкості транзакцій.
Зниження навантаження на систему автентифікації. SSO зменшує кількість запитів на автентифікацію, які система має обробляти, тим самим підвищуючи загальну продуктивність системи.	Потенційні ризики безпеки при неправильній реалізації. Неправильна конфігурація SSO може призвести до вразливостей, які зловмисники можуть використати для обходу механізмів автентифікації.

Блокчейн як засіб забезпечення надійності автентифікації

Останнім часом технологія блокчейн активно розглядається як потенційне рішення для підвищення надійності процесів автентифікації користувачів в інтернеті. Блокчейн з його децентралізованою природою, криптографічним захистом і прозорими транзакціями може забезпечити більш безпечний та надійний спосіб перевірки особи користувача [6].

Одним з ключових напрямків застосування блокчейну для автентифікації є зберігання і управління цифровими ідентифікаторами. Блокчейн дозволяє створити децентралізований реєстр унікальних ідентифікаторів, якими володіють і управляють користувачі. Ці ідентифікатори можуть використовуватися для надійної автентифікації в різних системах та сервісах [7]. Розподілена природа блокчейну означає, що компрометація окремих вузлів не призведе до витоку чи втрати ідентифікаційних даних.

ISSN 2663 - 4023

Рис. 1. Схематичне зображення облікового запису, який можна перевірити, і презентації, яку можна перевірити

Емітент підписує обліковий запис, який можна перевірити, для користувача, а потім публікує його підтвердження в блокчейні. Пізніше користувач створює верифіковану презентацію і представляє її верифікатору. Верифікатор може перевірити презентацію на основі доказу облікового запису в блокчейні.

Іншим важливим аспектом є можливість використання криптографії на блокчейні для створення цифрових підписів. Цифровий підпис, заснований на закритому ключі користувача, може слугувати надійним підтвердженням його особи. Поєднання цифрових підписів з ідентифікаторами на блокчейні створює міцну основу для автентифікації [8].

Додатково, блокчейн дозволяє реалізувати такі механізми, як нульове розкриття інформації, коли перевірка особи відбувається без передачі власне персональних даних. Це допомагає уникнути ризиків компрометації чутливої інформації під час автентифікації. Блокчейн також забезпечує прозорий запис всіх транзакцій, що надає можливості аудиту та аналізу процесів автентифікації [9].

Блокчейн може бути інтегрований в існуючі системи автентифікації для підвищення їх надійності. Наприклад, компанії можуть використовувати приватні блокчейн-мережі для безпечного зберігання ідентифікаційних даних своїх користувачів та надавати їм контрольований доступ до ресурсів. Застосування смарт-контрактів на блокчейні також дозволяє автоматизувати перевірку особи та надання доступу.

Звичайно, існують і певні виклики в застосуванні блокчейну для автентифікації. Це питання масштабованості, інтеграції з існуючими системами, нормативно-правового регулювання. Проте загалом блокчейн демонструє значний потенціал для побудови більш стійких і надійних систем автентифікації завдяки своїй децентралізованій архітектурі та криптографічному захисту [10].

Застосування смарт-контрактів для автоматизації процесів аутентифікації

Смарт-контракти на блокчейні надають цікаві та потужні можливості для автоматизації та значного підвищення ефективності процесів автентифікації користувачів. Смарт-контракт являє собою фрагмент коду, який автоматично виконується при настанні певних заздалегідь визначених умов в блокчейн-мережі. Цю перспективну технологію можна використати для створення повністю автономних систем перевірки особи користувача та надання йому доступу до ресурсів чи сервісів відповідно до результатів такої перевірки [6].

Одним з ефективних варіантів реалізації є створення смарт-контракту, який при отриманні запиту на автентифікацію користувача автоматично звертається до блокчейн-

мережі для перевірки унікального ідентифікатора цього користувача та його цифрового підпису, які були попередньо занесені до блокчейну. Якщо ідентифікатор та цифровий підпис є чинними і коректно верифікуються, смарт-контракт відразу ж надає користувачу доступ до запитуваного ресурсу чи сервісу повністю автономно, без необхідності будь-якого втручання людини.

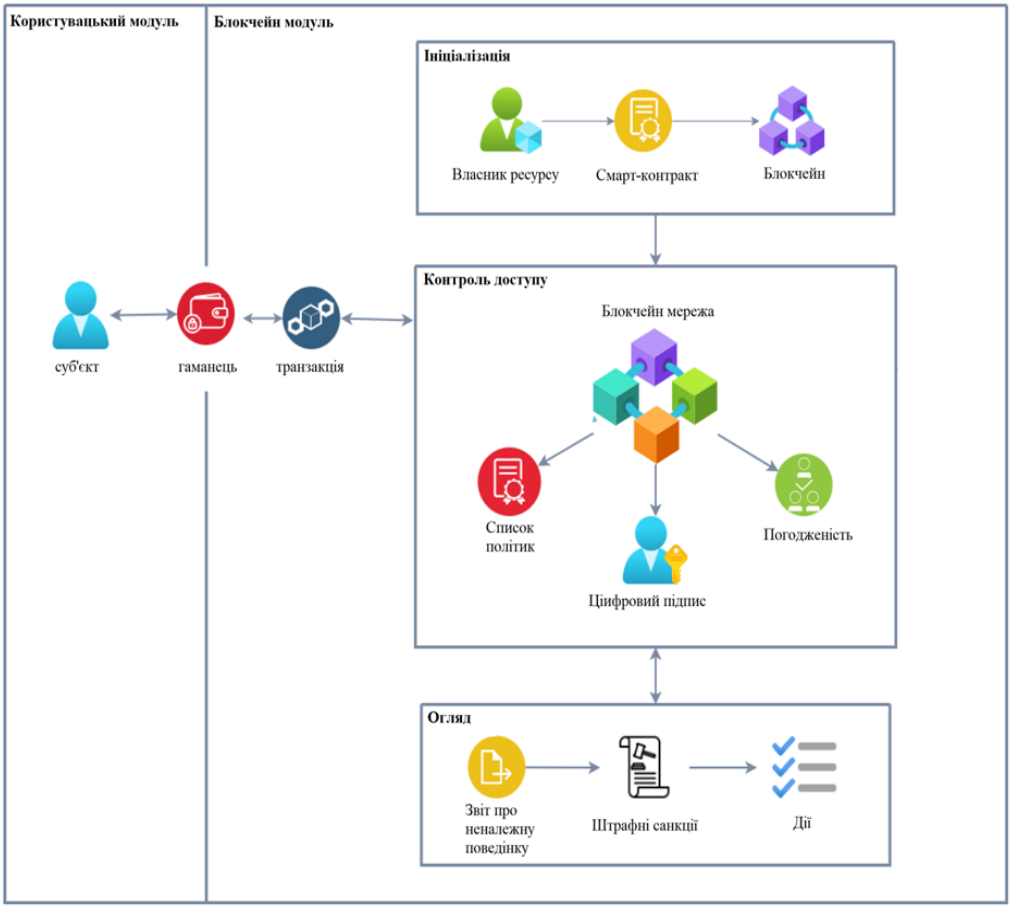

Рис. 2. Огляд запропонованої системи контролю доступу

Такий підхід дозволяє практично миттєво обробляти величезну кількість запитів на автентифікацію, оскільки весь процес від початку і до кінця відбувається автоматично відповідно до заздалегідь прописаної логіки смарт-контракту. Це також повністю усуває ймовірність помилок з боку людини під час перевірки даних чи прийняття рішення про надання доступу [6].

Більше того, логіка смарт-контракту може бути розширена для виконання набагато більш складних і різноманітних умов автентифікації, не обмежуючись простою перевіркою ідентифікатора та підпису користувача. Наприклад, смарт-контракт може бути запрограмований на перевірку репутації користувача, аналіз його попередньої активності в системі, перевірку наявності у користувача певних специфічних атрибутів, ролей, дозволів тощо [7]. Це надає практично необмежені можливості для реалізації найрізноманітніших складних політик контролю доступу та автентифікації.

Звичайно, застосування смарт-контрактів для автоматизації процесів автентифікації користувачів вимагає дуже обережного і відповідального підходу, особливо з точки зору забезпечення належного рівня безпеки. Адже смарт-контракти фактично мають повний

контроль над наданням доступу до системи. Тому вкрай важливо передбачити надійні механізми своєчасного оновлення та виправлення можливих уразливостей у коді смарт-контрактів, щоб уникнути їх несанкціонованого використання зловмисниками [8].

Ще одним критично важливим моментом є безпечне зберігання та використання криптографічних ключів, які надають доступ до виконання смарт-контрактів. Адже компрометація цих ключів зловмисником може мати катастрофічні наслідки та призвести до повної втрати контролю над системою автентифікації [8].

Проте, незважаючи на певні виклики та ризики, які обов'язково потрібно брати до уваги, технологія смарт-контрактів в цілому демонструє дійсно величезний потенціал для автоматизації і значного підвищення ефективності процесів автентифікації користувачів на блокчейні. За умови належної уваги до безпеки, смарт-контракти можуть стати одним з ключових технологічних елементів майбутніх децентралізованих систем ідентифікації та контролю доступу до цифрових ресурсів [9].

Важливим кроком є впровадження «Zero-Knowledge Proof». Використання «Zero-Knowledge Proof» чи інших криптографічних методів дозволяє доводити автентичність без передачі самої інформації. Це може бути корисним для перевірки ідентичності без розкриття деталей. Технологія блокчейн дозволяє створювати журнали подій, які є невідредагованими та доступними для аудиту. Це допомагає в управлінні та визначенні, хто, коли і як отримував доступ до персональних даних.

Протидія кіберзагрозам через децентралізовану автентифікацію

Децентралізована природа блокчейну та можливості його застосування для автентифікації користувачів можуть значно посилити захист від сучасних кіберзагроз. На відміну від традиційних централізованих систем, де всі дані зосереджені в єдиному місці, розподілена топологія блокчейну істотно ускладнює для зловмисників спроби атаки та компрометації системи [6].

Використання блокчейну як основи децентралізованої системи ідентифікації дозволяє досягти стійкості та безпеки завдяки розподіленню персональних даних користувачів у зашифрованому вигляді між величезною кількістю незалежних вузлів [7]. За такої моделі компрометація частини вузлів не призведе до витоку критичних конфіденційних даних або виведення з ладу всієї системи в цілому.

Додаткові механізми, такі як багатофакторна автентифікація на основі асиметричних криптографічних ключів користувача, суттєво ускладнюють спроби підбору даних для несанкціонованого доступу до системи. Використання смарт-контрактів на блокчейні дає змогу гнучко налаштувати розвинені політики безпеки та контролю доступу для різних ролей користувачів [8], [9].

Блокчейн-базована децентралізована автентифікація також є стійкою до таких поширених атак, як фішинг чи перехоплення сесії, оскільки в такій моделі відсутня необхідність передавати паролі користувача через мережу в процесі авторизації. Зловмиснику вкрай складно підробити чи перехопити дані для входу, що ґрунтуються на криптографічних ключах [10].

Практичне застосування блокчейну в автентифікації

Безпека облікових записів через блокчейн

Технологія блокчейн пропонує альтернативний підхід для безпечного зберігання даних про користувачів. Завдяки децентралізованому та незмінному характеру блокчейну, дані розподіляються між багатьма вузлами мережі та захищені криптографічно [6].

Один з підходів полягає у використанні блокчейну як основи для створення децентралізованих ідентифікаторів (DIDs). DID дозволяє користувачам контролювати та володіти власними даними для автентифікації [13]. Ці ідентифікатори можуть бути пов'язані з обліковими даними, збереженими в блокчейні.

Іншим варіантом є хешування та зберігання облікових даних безпосередньо в блокчейні. Це гарантує цілісність та неможливість непомітного редагування [14]. При цьому, актуальні дані можуть зберігатися окремо і лише їх хеш — у блокчейні.

Отже, блокчейн надає нові інструменти для підвищення захисту облікових даних через децентралізацію, криптографічний захист та можливості контролю користувача над власними даними.

Розподілена система логування доступу

В контексті систем управління доступом, таких як SSO, системи логування дій користувачів відіграють вирішальну роль, дозволяючи виявляти неавторизовані дії за допомогою аналізу аномальної поведінки, незвичайних дій або місць доступу [15]. Це ключово для ідентифікації потенційних атак [14]. Проте, системи логування можуть бути ціллю атак, наприклад, CAPEC-161, що включає маніпуляції з інфраструктурою системи, та CAPEC-268, що спрямовані на маніпуляції з журналами аудиту [16], [17]. Основна мета таких атак — змінити записи журналу, щоб приховати неавторизовані дії, включаючи видалення, зміну або додавання фальшивих записів, а також придушення логування.

Застосування блокчейн-технології може значно підвищити захищеність систем логування. Властивість незмінності даних у блокчейні забезпечує, що збережені записи залишаються недоторканими: не видалені, не змінені та не доповнені несанкціоновано [16], [17]. Це досягається через використання хешів для кожного блоку, де зміна даних у будь-якому блоку веде до зміни хешу, що легко виявити, оскільки кожен наступний блок зберігає хеш попереднього.

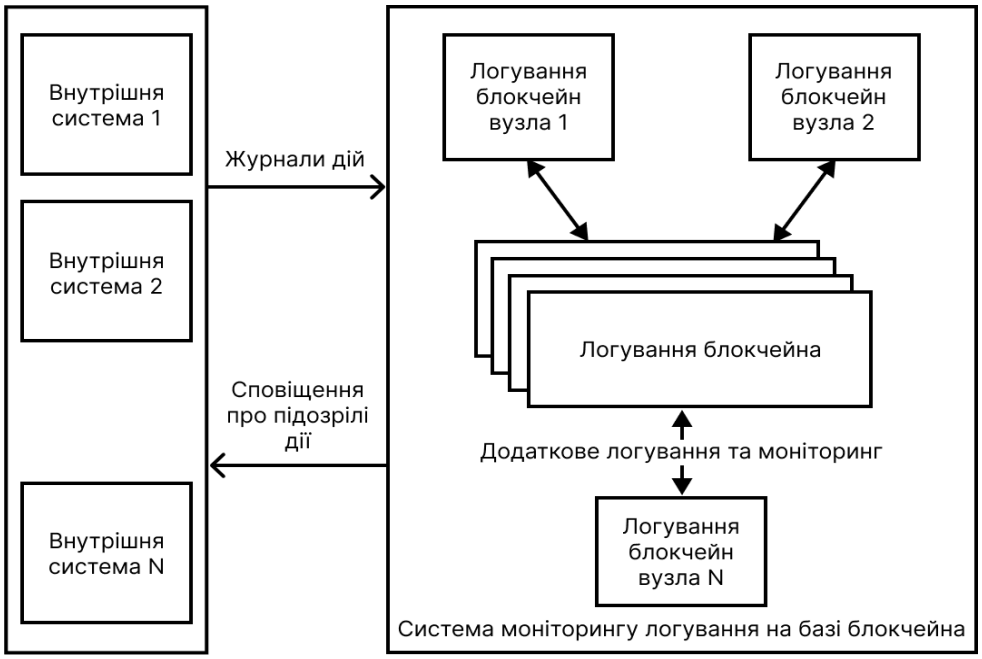

Рис. 3. Концепція системи моніторингу на основі блокчейн

Такий підхід до моніторингу, представлений на рис. 3, забезпечує високий рівень безпеки даних.

Незважаючи на переваги, пов'язані з незмінністю та безпекою, блокчейн вносить певні обмеження. Зокрема, збільшення обсягу даних у блокчейні може призвести до збільшення його розміру, що, у свою чергу, може уповільнити обробку та зменшити швидкість виконання системи через збільшення часу на досягнення консенсусу [16], [17]. Проте, великий розмір блокчейну також збільшує стійкість системи до атак, оскільки будь-які спроби несанкціонованих змін вимагають значних обчислювальних ресурсів, що робить такі атаки менш вигідними для зловмисників.

Захист ідентичності через блокчейн

В контексті блокчейну псевдоанонімність означає те, що облікові дані користувача та його цифровий ідентифікатор не пов'язані між собою безпосередньо, проте їх можна пов'язати використовуючи різні методи та засоби для цього. Відповідно існують різні блокчейн проєкти [18] які використовують складніші криптографічні методи та засоби для забезпеченням більшої приватності користувачі.

Огляд запропонованої технології над іншими наведено у табл. 2.

Таблиця 2

Переваги використання запропонованої технології над іншими

Перевага	Опис
Відсутність центральної точки вразливості	Децентралізована структура блокчейну виключає єдину точку відмови, що значно знижує ризики кібератак.
Рівноправність вузлів в мережі	Кожен вузол має однакові права і можливості, що сприяє демократизації управління даними та контролем доступу.
Можливість безпечного зберігання даних про користувачів	Дані про користувачів зберігаються в зашифрованому вигляді та розподілені по мережі, що підвищує безпеку інформації.
Анонімізація даних для входу	Система використовує унікальні ідентифікатори без прямого вказівки на особисті дані, що забезпечує приватність користувачів.
Зниження навантаження на мережу	Використання спеціалізованих блокчейнів для зберігання облікових даних та логування активності оптимізує ресурси мережі.
Відсутність можливості несанкціонованих змін у логах дій	Незмінність записів у блокчейні гарантує, що історія активності користувачів залишиться недоторканною і перевіреною, що важливо для аудиту та відповідальності.

Однак, в контексті розробки системи SSO дана властивість технології може стати одним з інструментів побудови системи логування. Аналіз діяльності користувачів в журналі активності та виявлення аномальної активності може свідчити про наявність несанкціонованих дій. Хоч і сама персона користувача не можу бути встановлена за наявністю лише криптоадреси користувача, наявність окремої бази даних із обліковими даними користувача дозволить встановити особу, яка, можливо, є порушником. В даному випадку псевдоанонімність полягає в тому, що всі дії логуються в журналі використовуючи лише криптадресу користувача, однак існує окремий захищений блокчейн який містить облікові дані самого користувача, та дозволяють встановити його особу у випадку необхідності. Очевидно, що даний спосіб застосування такої властивості є неоднозначним, оскільки він не гарантує повну анонімність користувачів систем та надає можливість встановити особу користувача, але це є необхідним заходом в разі застосування SSO на основі блокчейну, оскільки це буде створювати для зловмисників всередині системи того, що їхню особу буде встановлено.

Гнучке управління правами доступу з блокчейном

Розмежування доступу є однією з ключових функціональних характеристик будь-якої системи керування доступом і SSO зокрема. Якщо в традиційних системах керування доступом відбувається на стороні системи, яка зберігає правила розмежування та відповідає їхнє виконання. При використанні блокчейну функцію зберігання дозволів можна перенести на самих користувачів системи, в той час коли виконання правил розмежування доступу та видачу нових дозволів залишити на стороні системи [19].

Для забезпечення такого підходу можна використати такі технології: NFT, Смарт-контракти та використання різних типів блокчейнів — відкритих, закритих, гібридних тощо.

Технологія блокчейн відкриває нові можливості для гнучкого управління правами доступу в системах керування доступом, зокрема в SSO. Завдяки використанню невзаємозамінних токенів (NFT) та смарт-контрактів з'являється змога автоматизувати процес надання та вилучення прав, зберігаючи цю інформацію в децентралізованому блокчейні. Кожен NFT може нести унікальну інформацію про права його власника, яку смарт-контракти можуть автоматично інтерпретувати для надання чи блокування доступу до певних частин системи. Наприклад, NFT може містити дані про права на читання, зміну або видалення певних даних чи документів. Смарт-контракт перевірятиме ці права і дозволить чи заблокує відповідні операції для даного користувача. Окремі інформаційні ресурси можна розмістити в різних блокчейнах залежно від необхідного рівня доступу. Наприклад, відкриті дані — в публічному блокчейні, внутрішня документація — у приватному блокчейні організації, а дані з обмеженим доступом — у консорціумному блокчейні. Хоча використання кількох блокчейнів і знижує децентралізацію системи в цілому, це дає значні переваги для гнучкого та безпечного керування правами в SSO. Окремо варто згадати можливості аудиту та контролю за наданням і вилученням прав доступу завдяки прозорості та незмінності транзакцій у блокчейні.Інтеграція NFT та смарт-контрактів дозволяє автоматизувати рутинні процеси надання і блокування доступу, позбавляючи адміністраторів необхідності вручну керувати цими правами. Система сама може верифікувати наявність потрібних NFT і приймати рішення про доступ відповідно до закладеної в смарт-контракт логіки [18].

Потенційні виклики

Рис. 4. Виклики при інтеграції блокчейн-логування і SSO

Сучасний підхід до систем одного входу (SSO) вимагає інноваційних рішень для забезпечення високого рівня безпеки, конфіденційності, і надійності. В цьому контексті, блокчейн пропонує унікальну вартість через свої основні властивості: децентралізацію, незмінність даних, і прозорість. Пропонуємо розробку системи SSO, яка використовує блокчейн не тільки для безпечного зберігання даних про користувачів та логів їх дій, але й для реалізації комплексних механізмів аутентифікації. Використання смарт-контрактів дозволяє автоматизувати процеси валідації прав доступу, забезпечуючи гнучкість та масштабованість системи. Ключовим аспектом є децентралізоване управління ідентифікаторами користувачів, що забезпечує високий рівень безпеки і знижує ризики централізованих атак. Незмінність даних в блокчейні відіграє критичну роль у виявленні та запобіганні кіберзагрозам, дозволяючи аудитувати логи дій користувачів в реальному часі для виявлення аномалій.

Важливим аспектом покращення безпеки систем аутентифікації є впровадження гнучкого управління правами доступу. Використання блокчейну дозволяє реалізувати модель, в якій кожен користувач має унікальний цифровий ідентифікатор, що зберігається в децентралізованому реєстрі. Це забезпечує вищий рівень безпеки порівняно з традиційними централізованими системами, де інформація про користувачів зберігається в одному місці, що робить її потенційною мішенню для зловмисників.

Смарт-контракти можуть бути використані для автоматизації процесів надання та відкликання прав доступу, роблячи систему більш ефективною та знижуючи ризик людських помилок. Крім того, використання невзаємозамінних токенів (NFT) для представлення прав доступу може забезпечити додатковий рівень безпеки та гнучкості, дозволяючи детально контролювати, які саме ресурси доступні кожному користувачу.

Ще одним напрямком підвищення безпеки є використання доказів з нульовим знанням. Ця технологія дозволяє користувачам доводити володіння певною інформацією без необхідності її розкриття. Наприклад, користувач може довести, що він знає пароль, не повідомляючи сам пароль. В контексті блокчейну, це може бути використано для створення систем аутентифікації, які забезпечують високий рівень приватності та безпеки. Використання децентралізованих ідентифікаторів (DID) дозволяє користувачам контролювати свою ідентифікаційну інформацію без необхідності залучення третіх сторін. Це забезпечує вищий рівень приватності та безпеки, оскільки інформація зберігається в розподіленій мережі замість централізованих баз даних, які можуть бути вразливими до хакерських атак.Для подальшого підвищення безпеки системи можна інтегрувати розширені методи аутентифікації, такі як біометричні дані або одноразові паролі, які генеруються в реальному часі. Ці методи можуть бути впроваджені через смарт-контракти, які автоматично перевірятимуть правильність аутентифікаційних даних перед наданням доступу до системи. Використання блокчейна для логування активності користувачів у системі SSO не лише забезпечує незмінність записів, але й дозволяє виконувати детальний аналіз даних для виявлення потенційних загроз або аномалій у поведінці користувачів. Це стає можливим завдяки прозорості та відкритості даних у блокчейні, що дозволяє системам безпеки ефективно відстежувати та аналізувати всі дії в мережі.

Інтеграція блокчейн-технологій у існуючі IT-інфраструктури вимагає подолання низки технічних викликів, серед яких:

- Сумісність із існуючими системами: Блокчейн-технології часто розробляються як автономні рішення, що може ускладнити їх інтеграцію з існуючими базами даних, системами управління контентом та іншими корпоративними додатками. Наприклад, компаніям може знадобитися

розробка спеціалізованих API або проміжного програмного забезпечення для забезпечення взаємодії між блокчейн-мережами та традиційними IT-системами.

- Масштабування: Однією з основних проблем блокчейну, особливо у публічних мережах, є масштабування. Наприклад, мережа Bitcoin може обробляти лише 7 транзакцій за секунду, а Ethereum — приблизно 30 транзакцій. Це обмеження створює проблеми для великих організацій, які потребують високої пропускної здатності для логування та інших операцій. Рішення, такі як Lightning Network для Bitcoin та шардінг для Ethereum, розробляються для вирішення цих проблем, але ще не були повністю інтегровані на момент мого останнього оновлення.
- Безпека та приватність: Хоча блокчейн вважається надзвичайно безпечною технологією, існують питання, пов’язані з приватністю даних, особливо в публічних блокчейн, де транзакції є відкритими для перегляду. Компанії повинні знайти баланс між використанням блокчейну для забезпечення прозорості та аудитабельності логів та забезпеченням конфіденційності та захисту особистих даних своїх користувачів. Рішення, такі як приватні блокчейни або використання технологій анонімізації транзакцій, можуть допомогти вирішити ці проблеми, але вони вимагають додаткових зусиль для інтеграції та управління.
- Управління ключами та доступом: Блокчейн вимагає від користувачів управління криптографічними ключами для здійснення транзакцій або доступу до інформації. Це створює виклики з безпеки, особливо у випадках втрати ключів користувачем або їх компрометації, що може призвести до незворотних втрат даних або доступу. Компаніям необхідно впровадити надійні механізми управління ключами та політики безпеки для забезпечення захисту ключів та контролю доступу.
- Інтероперабельність блокчейнів: Для організацій, які хочуть використовувати декілька блокчейн-мереж або інтегрувати блокчейн-логування з іншими блокчейн-базованими додатками, інтероперабельність стає ключовим викликом. Наразі більшість блокчейн-платформ функціонують як закриті системи з обмеженою здатністю до взаємодії. Розробка стандартів та протоколів для інтероперабельності між різними блокчейнами є активною областю дослідження, але практична інтеграція все ще залишається складним завданням.
- Оновлення та сумісність версій: Блокчейн-платформи постійно розвиваються, і випуск нових версій може створити виклики зі сумісністю, особливо для розробників додатків та служб, що залежать від конкретних функцій або інтерфейсів блокчейна. Організаціям необхідно забезпечити регулярне оновлення своїх систем і адаптацію до змін в блокчейн-екосистемах, що може вимагати значних ресурсів та планування.
- Виклики зберігання даних: Хоча блокчейн забезпечує високий рівень безпеки для зберігання даних, він також може створити виклики з ефективністю зберігання, особливо у випадку великих об’ємів даних. Логування та зберігання великої кількості даних у блокчейні може бути неефективним та дорогим через реплікацію даних у всій мережі. Використання off-chain рішень або гібридних підходів, де тільки хеші даних

зберігаються у блокчейні, може допомогти оптимізувати витрати та ефективність зберігання.

Організаційні виклики, пов'язані з інтеграцією блокчейн-логування та систем SSO, охоплюють широкий спектр аспектів, від управління змінами до розвитку навичок. Ось детальніше про кожен із них:

- Управління змінами та корпоративна культура: Впровадження нових технологій, як-от блокчейн та SSO, часто вимагає значних змін у корпоративних процесах і робочих звичках. Це може зіткнутися з опором з боку співробітників, які можуть бути незадоволені відходом від звичних методів роботи. Організаціям необхідно інвестувати у програми управління змінами, щоб сприяти адаптації персоналу, зокрема через тренінги, семінари та підтримку з боку керівництва.
- Навчання та розвиток навичок: Технології блокчейн та SSO є відносно новими і складними, що вимагає від співробітників відповідних технічних знань і навичок. Організаціям потрібно забезпечити доступ до ресурсів для навчання та професійного розвитку, включаючи спеціалізовані курси та сертифікації, щоб персонал міг ефективно працювати з новими системами.
- Рекрутинг та залучення талантів: Враховуючи високий попит на спеціалістів у галузі блокчейну, знайти кваліфікованих працівників може бути складно. Організаціям доводиться конкурувати за таланти не тільки з іншими компаніями у своїй галузі, але й зі стартапами та технологічними гігантами. Це може вимагати перегляду пакетів компенсацій, робочого середовища та можливостей для кар'єрного росту, щоб залучити та утримати найкращі кадри.
- Організаційна структура та процеси: Інтеграція блокчейну та SSO може вплинути на існуючі бізнес-процеси та організаційну структуру. Наприклад, може знадобитися створення нових відділів або ролей, зосереджених на управлінні блокчейн-ініціативами або кібербезпекою. Організації мають ретельно планувати ці зміни, щоб забезпечити плавну інтеграцію нових систем без негативного впливу на поточні операції.
- Відповідність регулятивним вимогам: Впровадження блокчейну та SSO також вимагає розуміння та відповідності регулятивним вимогам, які можуть варіюватися в залежності від галузі та регіону діяльності. Організаціям потрібно працювати з юридичними та відділами з питань відповідності, щоб забезпечити, що нові технології не порушують існуючі закони та нормативи, особливо у сферах захисту даних та фінансового регулювання.

При інтеграції блокчейн-логування та систем SSO в механізми кібербезпеки виникають специфічні виклики безпеки, які потребують особливої уваги:

- Захист криптографічних ключів: В умовах блокчейну безпека користувача залежить від приватних ключів, що використовуються для підписання транзакцій. Втрата або компрометація цих ключів може призвести до незворотної втрати доступу до активів або даних. Забезпечення безпеки зберігання та управління ключами стає критичним аспектом, що вимагає впровадження надійних механізмів управління ключами (KMS) та багатофакторної аутентифікації.
- Вразливості смарт-контрактів: Смарт-контракти, які автоматично виконують умови угоди на основі коду, є фундаментальною частиною

багатьох блокчейн-платформ. Проте, вони можуть містити помилки або вразливості, що відкриває потенціал для атак. Відомий випадок DAO (Decentralized Autonomous Organization) на Ethereum, де вразливість у смарт-контракті призвела до втрати мільйонів доларів, яскраво демонструє ризики, пов'язані з безпекою смарт-контрактів.

- Фішинг та соціальна інженерія: Зловмисники часто використовують фішинг та інші методи соціальної інженерії для отримання доступу до користувацьких облікових записів або приватних ключів. В умовах SSO, де один набір облікових даних дає доступ до декількох сервісів, успішна фішингова атака може мати особливо руйнівні наслідки, забезпечуючи зловмисникам доступ до широкого спектру ресурсів жертви.
- Відмова в обслуговуванні (DDoS): Блокчейн-мережі, особливо публічні, можуть стати мішенями для атак типу відмови в обслуговуванні, спрямованих на перевантаження мережі великою кількістю транзакцій або запитів. Хоча децентралізована природа блокчейну робить його більш стійким до таких атак у порівнянні з традиційними централізованими системами, великі та координовані DDoS-атаки все ще можуть спричинити значні збої в роботі.
- Проблеми з приватністю: Хоча блокчейн забезпечує високий рівень безпеки через криптографію та децентралізацію, він також створює унікальні виклики для приватності. Публічні блокчейни зберігають транзакції відкрито, що може призвести до небажаного розкриття інформації. Організаціям потрібно знайти баланс між використанням блокчейну для забезпечення прозорості та захистом конфіденційності даних.

Загалом при використання технології блокчейн в системах SSO слід розглядати її як можливе доповнення до існуючої системи, а не як альтернативу традиційним системам. Зокрема, наявність блокчейн версії журналу подій може стати захищеною альтернативою звичайним журналам доступу, оскільки такий журнал буде захищеним від несанкціонованого втручання в записи журналу, що унеможливлює можливість приховування аномальних дій в мережі, що дозволить простіше виявляти порушника. Або використання блокчейну як сховище облікових даних користувачів, що може спростити обмін між різними установами та усуне необхідність багаторазового дублювання даних про користувачів, вносити зміни в них в одному місці, а самим користувачам — контролювати ці зміни, та бачити сторону яка їх змінювала. Використання технології блокчейн на даному етапі її розвитку можна розглядати як експериментальне доповнення до існуючих систем та як основу для подальших досліджень даної теми [20].

Смарт-контракти автоматизують виконання угод в блокчейні, забезпечуючи виконання певних умов без участі третіх сторін. Однак, вони можуть містити вразливості або помилки у коді, що створює ризики безпеки. Ось як можна мінімізувати ці ризики:

- **Аудит смарт-контрактів.** Залучення зовнішніх аудиторів: Регулярний аудит коду смарт-контрактів професійними аудиторами або компаніями, спеціалізованими на безпеці блокчейна, може виявити потенційні вразливості або помилки в логіці, які можуть бути виправлені перед розгортанням на основній мережі. Використання перевірених шаблонів: Опирання на стандартизовані та вже перевірені шаблони смарт-контрактів може знизити ризик помилок у коді, адже ці шаблони вже були аудитовані та випробувані спільнотою.

- **Тестування.** Розробка тестових сценаріїв: Створення комплексних тестових сценаріїв, які імітують різноманітні умови використання та атаки, для перевірки надійності та безпеки смарт-контрактів. Використання тестових мереж: Розгортання смарт-контрактів у тестових мережах (наприклад, Ropsten для Ethereum) перед їх впровадженням в основну мережу дозволяє виявити та виправити помилки в безпечному середовищі.
- **Автоматизовані інструменти аналізу.** Використання інструментів статичного та динамічного аналізу: Автоматизовані інструменти можуть допомогти виявити вразливості у коді смарт-контрактів, наприклад, відомі патерни атак або помилки управління пам'яттю. Застосування фаззінгу: Фаззінг (випадкове генерування вхідних даних) може виявити непередбачені вразливості або помилки в коді, які не були покриті стандартними тестами.
- **Освітні програми для розробників.** Підвищення кваліфікації розробників: Проведення регулярних тренінгів та воркшопів для розробників смарт-контрактів, щоб ознайомити їх з найкращими практиками безпеки, відомими вразливостями та методами їх запобігання.
- **Реагування на інциденти.** План реагування на інциденти: Розробити та впровадити чіткий план реагування на інциденти для швидкого виявлення, аналізу та виправлення помилок у смарт-контрактах після їх виявлення. Застосування цих рекомендацій допоможе забезпечити вищий рівень безпеки смарт-контрактів, мінімізувати ризики втрат або зловмисного використання активів і даних, а також підвищити довіру користувачів та інвесторів до блокчейн-платформ і додатків.

ВИСНОВКИ

Дослідження виявило, що блокчейн пропонує унікальні механізми захисту даних через децентралізацію та криптографію, що забезпечує безпеку, надійність, і прозорість у процесах логування та аутентифікації. Це підкреслює роль блокчейна як засобу забезпечення довіри між сторонами без необхідності централізованого посередника.

Виявлено, що багато існуючих систем страждають від слабких місць, які можуть бути використані для несанкціонованого доступу. Блокчейн може вирішити ці проблеми за допомогою розподілених реєстрів та смарт-контрактів, підвищуючи цим безпеку та ефективність.

Дослідження ідентифікує ключові проблеми, пов'язані з кіберзагрозами, як-от фішинг, витоки даних, та інші форми кібератак. Блокчейн пропонує механізми для мінімізації цих ризиків через незмінність даних та використання розподілених систем.

Оцінка показала, що використання блокчейну може значно підвищити стійкість систем логування та аутентифікації до кібератак, забезпечуючи ефективний захист даних та ідентифікаційної інформації.

Пропонується інноваційний підхід до інтеграції блокчейн технологій у системи аутентифікації та логування, що включає розробку нових протоколів для забезпечення безпеки та приватності, а також створення ефективних механізмів управління доступом.

Загалом, впровадження блокчейну в технологію SSO може відкрити нові можливості для створення безпечного, надійного та інноваційного інтернет-середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Benjamin, N. (2021). How Effective Is Blockchain in Cybersecurity? *Measurement: ISACA Journal, 4.*
2. Moosavi, N., & Taherdoost, H. (2023). Blockchain Technology Application in Security: A Systematic Review. *Blockchains, 1(2),* 58–72. https://doi.org/10.3390/blockchains1020005
3. Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity Challenges in Blockchain Technology: A Scoping Review. *Human Behavior and Emerging Technologies 2022,* 1–11. https://doi.org/10.1155/2022/7384000
4. Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. *Front. Blockchain, 3.* https://doi.org/10.3389/fbloc.2020.00026
5. Feng, Y., Zhong, Z., Sun, X., Wang, L., Lu, Y., & Zhu, Y. (2023). Blockchain enabled zero trust based authentication scheme for railway communication networks. *Journal of Cloud Computing, 12.* https://doi.org/10.1186/s13677-023-00411-z
6. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data (BigData Congress),* 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
7. Özyılmaz, K. R., & Yurdakul, A. (2017). Designing a blockchain-based IoT infrastructure with erlang. *IEEE Globecom Workshops (GC Wkshps*). https://doi.org/10.1109/GLOCOMW.2017.8269080
8. Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2019). Security and Privacy Preservation in Blockchain-Based Crowdsourcing Services. *IEEE Network, 33(6),* 180–186. https://doi.org/10.1109/MNET.001.1900015
9. Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly, 38(8),* 1710–1732. https://doi.org/10.1080/01436597.2017.1298438
10. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36,* 55–81. https://doi.org/10.1016/j.tele.2018.11.006
11. Hunt, T. (2017). *LinkedIn Breach from 2012 Affected 700 Million Users*.
12. Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy, 16(4),* 20–29.
13. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet, 10(2),* 20.
14. Vujičić, D., Jagodić, D., & Ranđić, S. (2018). Blockchain technology, bitcoin, and ethereum: A brief overview. *17th International Symposium INFOTEH-JAHORINA (INFOTEH),* 1–6.
15. Ezawa, Y., et al. (2019). Designing Authentication and Authorization System with Blockchain. *14th Asia Joint Conference on Information Security (AsiaJCIS),* 111–118.
16. Ao, W., Fu, S., Zhang, C., Huang, Y., & Xia, F. (2019). A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography. *IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET),* 90–95.
17. *MultiChain | Enterprise blockchain platform*. (n.d.). MultiChain | Enterprise blockchain platform. https://www.multichain.com/
18. Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics and Applications. *11th IADIS International Conference on Information Systems,* 49–57.
19. Poberezhnyk, V., Opirskyy, I. (2023). Developing of Blockchain Method in Message Interchange Systems. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421,* 148–157.
20. Poberezhnyk, V., Balatska, V., Opirskyy, I. (2023). Development of the Learning Management System Concept based on Blockchain Technology. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, Vol. 3550,* 143–156.

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

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

Petro Petriv
Postgraduate of the Department of "Information Security"
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0000-7426-3696
petro.p.petriv@lpnu.ua

EFFECTIVENESS OF BLOCKCHAIN LOGGING AND SSO IN CYBER SECURITY MECHANISMS

Abstract. With the rise of cyber threats in the era of digital transformation, protecting information systems becomes crucial for ensuring data reliability and security. This is especially true for authentication and logging systems, which are key elements in identifying and countering unauthorized access. The use of identical credentials and traditional authentication methods opens up wide opportunities for cybercriminals. This article explores the use of blockchain technology as a means to combat cyber threats through the implementation of immutable, decentralized logging and authentication systems. Blockchain offers unique advantages, such as data immutability and distributed storage, which can significantly complicate unauthorized interference in security systems. Current trends in the field of cybersecurity are examined, particularly the challenges associated with data compromise and ineffective information exchange between systems. An important part of the article is the analysis of recent research focused on the capabilities of blockchain in the development of identification and authentication systems based on decentralized identifiers and the integration of consensus technologies. The main goal of the research is to identify and develop technological solutions aimed at enhancing the security, resilience, and efficiency of logging and authentication systems through the application of blockchain. Additionally, innovative approaches to identification and authentication that can strengthen protection against cyber threats are considered.

Keywords: blockchain; cyber security; authentication; logging; decentralized identities; consensus technologies; NFT; cyber threats.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Benjamin, N. (2021). How Effective Is Blockchain in Cybersecurity? *Measurement: ISACA Journal, 4.*
2. Moosavi, N., & Taherdoost, H. (2023). Blockchain Technology Application in Security: A Systematic Review. *Blockchains, 1(2),* 58–72. https://doi.org/10.3390/blockchains1020005
3. Mahmood, S., Chadhar, M., & Firmin, S. (2022). Cybersecurity Challenges in Blockchain Technology: A Scoping Review. *Human Behavior and Emerging Technologies 2022,* 1–11. https://doi.org/10.1155/2022/7384000
4. Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. *Front. Blockchain, 3.* https://doi.org/10.3389/fbloc.2020.00026
5. Feng, Y., Zhong, Z., Sun, X., Wang, L., Lu, Y., & Zhu, Y. (2023). Blockchain enabled zero trust based authentication scheme for railway communication networks. *Journal of Cloud Computing, 12.* https://doi.org/10.1186/s13677-023-00411-z
6. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data (BigData Congress),* 557–564. https://doi.org/10.1109/BigDataCongress.2017.85
7. Özyılmaz, K. R., & Yurdakul, A. (2017). Designing a blockchain-based IoT infrastructure with erlang. *IEEE Globecom Workshops (GC Wkshps*). https://doi.org/10.1109/GLOCOMW.2017.8269080

8. Hu, P., Ning, H., Qiu, T., Song, H., Wang, Y., & Yao, X. (2019). Security and Privacy Preservation in Blockchain-Based Crowdsourcing Services. *IEEE Network, 33(6),* 180–186. https://doi.org/10.1109/MNET.001.1900015
9. Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? *Third World Quarterly, 38(8),* 1710–1732. https://doi.org/10.1080/01436597.2017.1298438
10. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36,* 55–81. https://doi.org/10.1016/j.tele.2018.11.006
11. Hunt, T. (2017). *LinkedIn Breach from 2012 Affected 700 Million Users.*
12. Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy, 16(4),* 20–29.
13. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? *Future Internet, 10(2),* 20.
14. Vujičić, D., Jagodić, D., & Ranđić, S. (2018). Blockchain technology, bitcoin, and ethereum: A brief overview. *17th International Symposium INFOTEH-JAHORINA (INFOTEH),* 1–6.
15. Ezawa, Y. et al. (2019). Designing Authentication and Authorization System with Blockchain. *14th Asia Joint Conference on Information Security (AsiaJCIS),* 111–118.
16. Ao, W., Fu, S., Zhang, C., Huang, Y., & Xia, F. (2019). A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography. *IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET),* 90–95.
17. *MultiChain | Enterprise blockchain platform*. (n.d.). MultiChain | Enterprise blockchain platform. https://www.multichain.com/
18. Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics and Applications. *11th IADIS International Conference on Information Systems,* 49–57.
19. Poberezhnyk, V., Opirskyy, I. (2023). Developing of Blockchain Method in Message Interchange Systems. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3421,* 148–157.
20. Poberezhnyk, V., Balatska, V., Opirskyy, I. (2023). Development of the Learning Management System Concept based on Blockchain Technology. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, Vol. 3550,* 143–156.