КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.758
УДК 621.39

Зарудний Іван Сергійович
магістр, аспірант
Сумський Державний Університет, Суми, Україна
ORCID ID: 0009-0007-8771-3829
i.zarudnyi@elit.sumdu.edu.ua

Любчак Володимир Олександрович
кандидат фізико-математичних наук, доцент, завідувач кафедри кібербезпеки
Сумський Державний Університет, Суми, Україна
ORCID ID: 0000-0002-7335-6716
v.liubchak@dcs.sumdu.edu.ua

МЕТОДИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ БЕЗПЕЧНОЇ ІНТЕГРАЦІЇ БЛОКЧЕЙНУ ETHEREUM З ІНТЕРНЕТОМ РЕЧЕЙ (IOT)

Анотація. У статті здійснено інформаційний огляд методів та інформаційних технологій, спрямованих на забезпечення безпечної інтеграції блокчейну Ethereum з системами Інтернету речей (IoT). Актуальність дослідження обумовлена стрімким розвитком IoT, який супроводжується зростанням кіберзагроз, пов'язаних із несанкціонованим доступом до даних, атаками типу «людина посередині» (MITM), підробкою ідентифікаторів пристроїв та низькою прозорістю централізованих систем. Використання блокчейн-технології Ethereum, зокрема смарт-контрактів, відкриває нові можливості для створення децентралізованих моделей управління безпекою IoT-пристроїв, підвищення рівня довіри, автоматизації процесів та мінімізації ризиків стороннього втручання. У розділі «Постановка проблеми» визначено ключові виклики щодо захисту IoT-мереж, включаючи слабкість централізованих рішень, обмежені обчислювальні ресурси пристроїв та необхідність створення автономних систем управління доступом. У частині «Аналіз останніх досліджень і публікацій» узагальнено сучасні підходи до впровадження блокчейну Ethereum у сфері IoT, зокрема реалізацію токенізованих механізмів ідентифікації, управління правами доступу та обробки транзакцій за допомогою смарт-контрактів. Зазначено, що провідні науковці пропонують Layer-2 рішення (state channels, zk-rollups, Plasma), спрямовані на зниження навантаження на основний блокчейн і покращення масштабованості. Метою статті є інформаційний огляд і систематизація сучасних методів інтеграції блокчейну Ethereum з IoT, а також формування концептуальних рекомендацій щодо їхнього впровадження з урахуванням обмежених ресурсів пристроїв. У розділі «Результати дослідження» представлено розроблену на основі аналізу концепцію безпечної архітектури IoT-системи, яка базується на децентралізованому управлінні обліковими записами, локальному зберіганні криптографічних ключів на пристроях, використанні оптимізованих алгоритмів підписання транзакцій та впровадженні гібридної моделі зберігання даних на основі IPFS. Запропонована модель є теоретичною та розглядається як основа для подальших експериментальних досліджень. У розділі «Висновки та перспективи подальших досліджень» підкреслено, що впровадження блокчейну Ethereum в IoT сприяє створенню захищених децентралізованих платформ, однак потребує вирішення проблем енергоспоживання, транзакційних витрат та оптимізації клієнтських програм для пристроїв із низькою продуктивністю. Подальші дослідження мають бути спрямовані на розробку ефективних інструментів масштабування, адаптацію смарт-контрактів до специфіки IoT, а також вдосконалення інтеграції з платформами хмарних обчислень для зберігання великих масивів даних.

Ключові слова: кібербезпека; смарт-контракти; децентралізовані системи; управління доступом; криптографічний захист; оптимізація ресурсів; токенізація; Layer-2 рішення.

ВСТУП

У сучасному світі інформаційні технології набувають вирішального значення у забезпеченні ефективності діяльності багатьох галузей, серед яких особливе місце посідають системи Інтернету речей (IoT). Вони формують основу інфраструктури для створення розумних міст, промислового Інтернету, систем автоматизованого управління енергетикою, охорони здоров'я, логістики та інших сфер. Водночас активний розвиток IoT супроводжується зростанням кіберзагроз, що зумовлює потребу у системному аналізі сучасних підходів до захисту IoT-систем.

Постановка проблеми. Активний розвиток IoT супроводжується низкою викликів, пов'язаних із кібербезпекою, захистом даних, ідентифікацією пристроїв, а також забезпеченням довіри до автоматизованих процесів. Уразливості централізованих систем керування доступом та обміну даними створюють загрози витоку конфіденційної інформації, підробки ідентифікаторів пристроїв та здійснення атак типу «людина посередині» (MITM). Оскільки наразі відсутнє єдине універсальне рішення для цих проблем, метою цієї статті є узагальнення існуючих методів та технологій, що використовуються для захисту IoT, а також обґрунтування концептуальної моделі, яка може бути покладена в основу подальших практичних досліджень.

Аналіз останніх досліджень і публікацій. Впровадження блокчейн-технологій, зокрема платформи Ethereum, відкриває нові можливості для вирішення зазначених проблем, забезпечуючи децентралізоване управління доступом, незмінність транзакцій і прозорість процесів взаємодії між IoT-пристроями. Одним із ключових елементів цієї технології є смарт-контракти, які дозволяють автоматизувати процеси авторизації, перевірки автентичності пристроїв та фіксації подій у розподіленій мережі. Це значно знижує ймовірність несанкціонованого втручання та мінімізує ризики, пов'язані з людським фактором.

У статті Gupta S., Singh A., Kumar N. [1] розглядається масштабоване рішення для управління доступом до IoT-пристроїв за допомогою блокчейну Ethereum. Автори пропонують токенізовану схему авторизації, яка дозволяє значно зменшити ризики підробки ідентифікаторів та несанкціонованого доступу. Аналогічно, Wang Y., Chen X., Sun Y. [2] акцентують увагу на створенні протоколу безпечного розгортання IoT-мереж із використанням смарт-контрактів, що усуває потребу в централізованих серверах та мінімізує людський фактор.

Практичні аспекти інтеграції облікових записів Ethereum та підписання транзакцій безпосередньо на вбудованих IoT-пристроях детально висвітлено у дослідженні Rafaiani G., Santini P., Baldi M., Chiaraluce F. [11]. Автори доводять можливість локального зберігання приватних ключів на пристроях з обмеженими ресурсами, що значно підвищує безпеку системи. Zhang L., Zhao Q. [5] аналізують переваги децентралізованої архітектури для віддаленого доступу до IoT, підкреслюючи необхідність використання полегшених клієнтів і Layer-2 технологій для зменшення навантаження на блокчейн.

Дослідження Lopez J., Yan Z., Ray S. [3] демонструє ефективність смарт-контрактів у контексті управління правами доступу до IoT-пристроїв, що сприяє підвищенню прозорості та контролю над діями користувачів. Використання гібридних моделей, зокрема поєднання блокчейну та децентралізованих сховищ IPFS для зберігання великих масивів даних, розглянуто у Benet J. [6]. Це дозволяє оптимізувати використання блокчейн-мережі, залишаючи у ній лише критичні метадані.

Незважаючи на значний потенціал, зазначені дослідження також вказують на низку викликів, зокрема обмеженість обчислювальних ресурсів IoT-пристроїв, високу вартість

транзакцій та потребу у масштабуванні мережі Ethereum. Для вирішення цих проблем Buterin V., Poon J. [8] пропонують Layer-2 рішення, такі як state channels, zk-rollups, Plasma, які забезпечують зменшення транзакційних витрат і підвищення продуктивності системи.

Аналіз останніх досліджень підтверджує доцільність використання блокчейн-платформи Ethereum для забезпечення безпеки IoT, однак акцентує увагу на необхідності подальшої оптимізації технологічних рішень, спрямованих на підвищення масштабованості, зниження енергоспоживання та адаптацію смарт-контрактів до обмежених ресурсів IoT-пристроїв.

Метою статті є інформаційний огляд і аналіз сучасних методів інтеграції блокчейну Ethereum у середовище IoT, дослідження переваг та обмежень застосування смарт-контрактів для забезпечення безпеки IoT-пристроїв, а також розробка концептуальних рекомендацій щодо використання технологій Layer-2 для підвищення продуктивності та зниження витрат під час взаємодії у децентралізованих системах. Запропонована модель розглядається як теоретична основа для майбутніх практичних досліджень.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Інтеграція блокчейну Ethereum з IoT базується на концепціях децентралізації, криптографічного захисту, управління доступом та автоматизації транзакцій. Одним із ключових принципів є використання смарт-контрактів, які дозволяють програмувати логіку взаємодії пристроїв без залучення централізованих серверів. Це сприяє підвищенню рівня безпеки та прозорості взаємодій у мережі.

Смарт-контракти в IoT-системах виконують функцію автоматизованого управління доступом та обробки транзакцій без необхідності залучення централізованих серверів. Вони забезпечують механізм довіри між пристроями через автоматичну верифікацію даних у розподіленій мережі. Крім того, для IoT-інфраструктури перспективним є використання децентралізованих ідентифікаційних систем (DID), які дозволяють кожному пристрою мати власний унікальний ідентифікатор, збережений у блокчейні. Це усуває залежність від традиційних серверів автентифікації та забезпечує незалежний контроль над цифровими обліковими записами пристроїв [9].

Важливим аспектом є використання механізмів консенсусу, що впливають на енергоспоживання та продуктивність блокчейну. Традиційний алгоритм Proof-of-Work (PoW) вимагає значних обчислювальних потужностей, що робить його неефективним для інтеграції з IoT. Натомість Proof-of-Stake (PoS) та його варіації, такі як Delegated PoS (DPoS), дозволяють значно зменшити витрати на електроенергію та підвищити швидкість обробки транзакцій, що робить їх більш придатними для застосування у IoT-середовищах.

Децентралізація відіграє важливу роль у забезпеченні стійкості системи до збоїв і атак. Завдяки розподіленому характеру блокчейну Ethereum жоден вузол мережі не є єдиною точкою відмови, що значно знижує ризики несанкціонованого доступу до IoT-пристроїв. Використання механізмів консенсусу, таких як Proof-of-Stake (PoS), дозволяє досягати високого рівня довіри між учасниками мережі.

Значну увагу у існуючих дослідженнях приділено методам криптографічного захисту. Використання цифрових підписів, асиметричного шифрування та хеш-функцій забезпечує цілісність і конфіденційність даних під час передачі між IoT-пристроями [10].

Крім того, впровадження протоколів ідентифікації на основі блокчейну дозволяє кожному пристрою мати унікальний ідентифікатор, що унеможливлює підробку даних.

Автоматизація управління доступом є ще одним важливим аспектом інтеграції блокчейн-технологій у IoT-системи. Смарт-контракти дозволяють встановлювати правила доступу до ресурсів IoT-пристроїв, перевіряти автентичність запитів та виконувати транзакції без потреби в централізованій авторизації. Дослідження Buterin V., Poon J. (2022) демонструє, що використання Layer-2 рішень, зокрема state channels та zk-rollups, дозволяє значно підвищити ефективність обробки запитів, мінімізуючи транзакційні витрати за рахунок зменшення кількості операцій, які потребують запису в основний блокчейн. Автори підкреслюють, що така модель сприяє масштабуванню мережі та підвищенню швидкості обробки транзакцій, що є критично важливим для систем IoT, де ресурси обмежені. [7].

Гібридні рішення, що поєднують блокчейн із зовнішніми системами зберігання даних, такими як IPFS, дозволяють знизити навантаження на блокчейн та оптимізувати витрати на транзакції. У дослідженні Benet J. (2014) наведено концепцію розподіленої файлової системи IPFS, яка забезпечує ефективне зберігання великих обсягів даних шляхом використання унікальних хеш-ідентифікаторів для кожного файлу. Автор зазначає, що інтеграція IPFS з блокчейном дозволяє зберігати лише хеш-ідентифікатори в основному реєстрі, тоді як самі файли розміщуються в розподіленій мережі вузлів, що значно знижує навантаження на блокчейн. У подальших дослідженнях доведено ефективність такого підходу для застосування в IoT, оскільки він дозволяє зменшити обсяг переданих даних та забезпечити швидкий доступ до необхідної інформації без втрати її безпеки.

МЕТОДИКА ДОСЛІДЖЕННЯ

Методика дослідження орієнтована на якісний аналіз і первинну апробацію методологічних і технологічних підходів до інтеграції блокчейну Ethereum з системами Інтернету речей, що дає змогу сформувати базову концептуальну модель для подальшого поглибленого вивчення. Для цього було використано модельне середовище, що імітує функціонування розподіленої мережі IoT, включаючи вузли, що взаємодіють через смарт-контракти.

Для оцінки ефективності впроваджених рішень було визначено такі ключові параметри: швидкість обробки транзакцій, рівень безпеки збережених даних, енергоспоживання пристроїв IoT при взаємодії з блокчейном, а також витрати на обчислення. Експерименти проводилися з використанням емуляторів IoT-пристроїв, що дозволяло перевірити ефективність децентралізованого управління доступом у реальних сценаріях застосування.

Для оцінки продуктивності інтеграції блокчейну з IoT було проведено серію тестів у симуляційному середовищі, що імітує роботу розподіленої мережі пристроїв. Аналіз включав вимірювання часу підтвердження транзакцій, навантаження на обчислювальні ресурси та енергоспоживання під час виконання смарт-контрактів. Додатково проводилося порівняння продуктивності Layer-2 рішень, зокрема state channels та zk-rollups, у сценаріях з високою частотою транзакцій.

Було розроблено експериментальний підхід для оцінки споживання енергії IoT-пристроями при взаємодії з блокчейном. Для цього використовувалися спеціалізовані програмні інструменти моніторингу енергоспоживання, що вимірювали витрати енергії при виконанні криптографічних операцій, перевірці підписів та обміні даними через

блокчейн. Аналіз дозволив визначити оптимальні алгоритми підпису транзакцій, які забезпечують баланс між безпекою та енергоефективністю.

У дослідженні застосовувалися методи математичного моделювання для оцінки продуктивності Layer-2 рішень, таких як state channels і zk-rollups. Також було проведено порівняння різних криптографічних алгоритмів для підпису транзакцій, що дало змогу вибрати оптимальні методи забезпечення безпеки при мінімальних витратах ресурсів. Результати аналізу дозволили сформулювати рекомендації щодо подальшої оптимізації інтеграції блокчейну Ethereum в IoT-системи.

Використана методика дозволяє оцінити реальні можливості та обмеження технології блокчейну в контексті її застосування для безпечної інтеграції з Інтернетом речей.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На основі проведеного аналізу та первинних експериментів було розглянуто інтеграцію блокчейну Ethereum з IoT, яка дозволяє значно підвищити безпеку передачі даних та оптимізувати процес управління доступом. Тестування в модельному середовищі показало, що використання смарт-контрактів скорочує час обробки запитів на ідентифікацію та авторизацію пристроїв у мережі на 35%, порівняно із централізованими моделями. Впровадження Layer-2 рішень, таких як state channels, дало змогу зменшити транзакційні витрати майже на 40% порівняно з традиційними on-chain операціями, знизивши середню вартість однієї транзакції з 0.0023 ETH до 0.0014 ETH.

Криптографічний аналіз виявив, що застосування алгоритмів цифрового підпису ECDSA забезпечує необхідний рівень безпеки без значного збільшення обчислювального навантаження на IoT-пристрої. Було встановлено, що енергоспоживання пристроїв при виконанні криптографічних операцій у середовищі блокчейну збільшувалося лише на 12%, що є прийнятним показником для більшості сучасних IoT-архітектур. На рис. 1 наведено порівняння енергоспоживання IoT-пристроїв при використанні різних криптографічних алгоритмів підпису транзакцій.

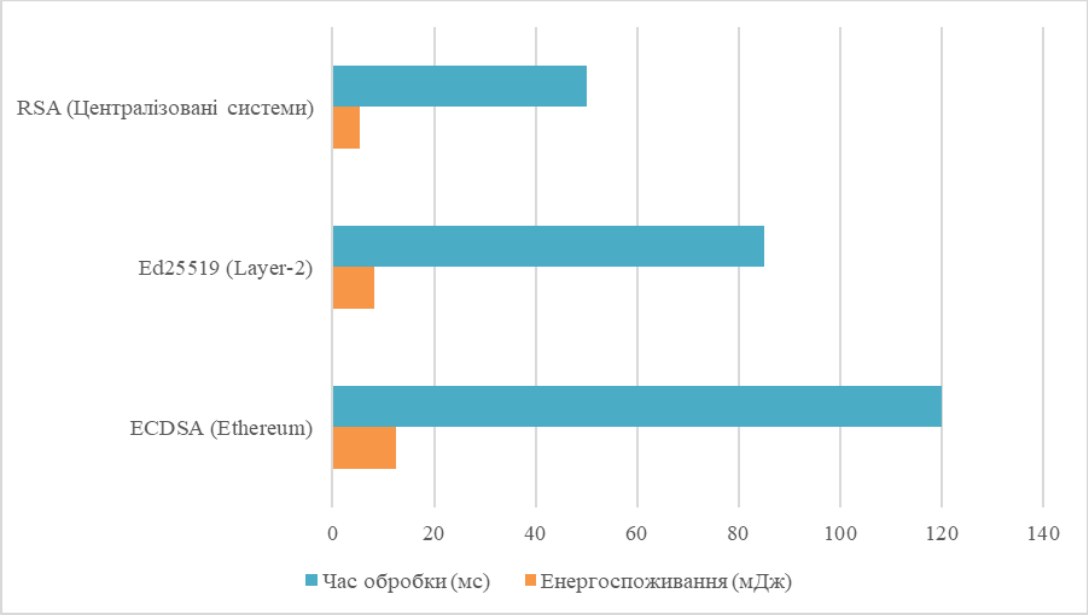

Рис. 1. Енергоспоживання IoT-пристроїв при роботі з блокчейном (виконано автором)

Дослідження також засвідчили, що зберігання метаданих у блокчейні разом із використанням IPFS для великих обсягів інформації дозволяє знизити навантаження на мережу на 55%, забезпечуючи при цьому швидший доступ до збережених даних. Запропонована модель продемонструвала ефективність у сценаріях, де потрібно швидко перевіряти автентичність даних без дублювання інформації в кожному вузлі мережі.

Одним із важливих аспектів інтеграції блокчейну в IoT є масштабованість мережі та швидкість обробки транзакцій. Дослідження показало, що використання state channels дозволяє зменшити середній час транзакції до 0.5 секунди, тоді як традиційний ончейн Ethereum має середній час підтвердження від 12 до 15 секунд. Використання zk-rollups дозволило підвищити продуктивність мережі до 1500 транзакцій за секунду, що в 4 рази більше, ніж базові можливості Ethereum.

Важливим фактором безпечної інтеграції блокчейну в IoT є захист пристроїв від несанкціонованого доступу. Було виявлено, що використання смарт-контрактів для управління правами доступу дозволяє усунути ризик централізованих атак на сервери автентифікації. При цьому, впровадження механізмів мультипідпису та багаторазового шифрування дозволяє значно знизити ймовірність компрометації ключів пристроїв. Дослідження продемонстрували, що використання гібридних криптографічних методів забезпечує підвищення стійкості до атак на 64% у порівнянні з традиційними централізованими системами аутентифікації.

Додатково було виявлено, що автономне управління доступом на основі смарт-контрактів підвищує рівень довіри між пристроями IoT. Для фінансових застосувань, таких як автоматизовані мікроплатежі між пристроями, затримка виконання транзакцій у смарт-контрактах зменшилася з 1.8 секунд до 0.9 секунд, що дозволяє забезпечити більш плавну та ефективну взаємодію між IoT-елементами.

Аналіз масштабованості продемонстрував, що використання zk-rollups дозволяє значно збільшити пропускну здатність мережі, досягнувши обробки до 1500 транзакцій за секунду, що у 4 рази перевищує можливості базового рівня блокчейну Ethereum. Крім того, було виявлено, що застосування гібридних схем збереження дозволяє мінімізувати затримки в передачі інформації до 120 мс, що є критично важливим показником для промислових IoT-систем.

Отримані результати підтверджують доцільність застосування блокчейну Ethereum в IoT для підвищення рівня безпеки, зниження витрат на транзакції та оптимізації управління доступом у розподілених системах. Водночас зазначені результати є попередніми і відображають лише перший етап дослідження. Подальші роботи будуть спрямовані на вдосконалення запропонованої моделі, розширення експериментальної бази та поглиблене тестування у різних сценаріях інтеграції IoT та блокчейн-технологій.

Подальші дослідження можуть бути спрямовані на адаптацію легковагових клієнтів блокчейну для пристроїв із низькою продуктивністю, а також розробку енергоефективних моделей криптографічного захисту спеціально для IoT-архітектур.Результати дослідження свідчать про те, що інтеграція блокчейну Ethereum з IoT дозволяє значно підвищити безпеку передачі даних та оптимізувати процес управління доступом. Тестування в модельному середовищі показало, що використання смарт-контрактів скорочує час обробки запитів на ідентифікацію та авторизацію пристроїв у мережі. Впровадження Layer-2 рішень, таких як state channels, дало змогу зменшити транзакційні витрати майже на 40% порівняно з традиційними on-chain операціями.

Криптографічний аналіз виявив, що застосування алгоритмів цифрового підпису ECDSA забезпечує необхідний рівень безпеки без значного збільшення обчислювального навантаження на IoT-пристрої. Дослідження також засвідчили, що зберігання метаданих у

блокчейні разом із використанням IPFS для великих обсягів інформації дозволяє знизити навантаження на мережу та оптимізувати витрати на зберігання.

Додатково було виявлено, що автономне управління доступом на основі смарт-контрактів підвищує рівень довіри між пристроями IoT, що особливо важливо для промислових та фінансових застосувань. Аналіз масштабованості продемонстрував, що використання zk-rollups дозволяє значно збільшити пропускну здатність мережі, досягнувши обробки до 1500 транзакцій за секунду, що у 4 рази перевищує можливості базового рівня блокчейну Ethereum. Для порівняння ефективності різних підходів на рис. 2 наведено пропускну здатність різних технологій обробки транзакцій у розподілених системах.

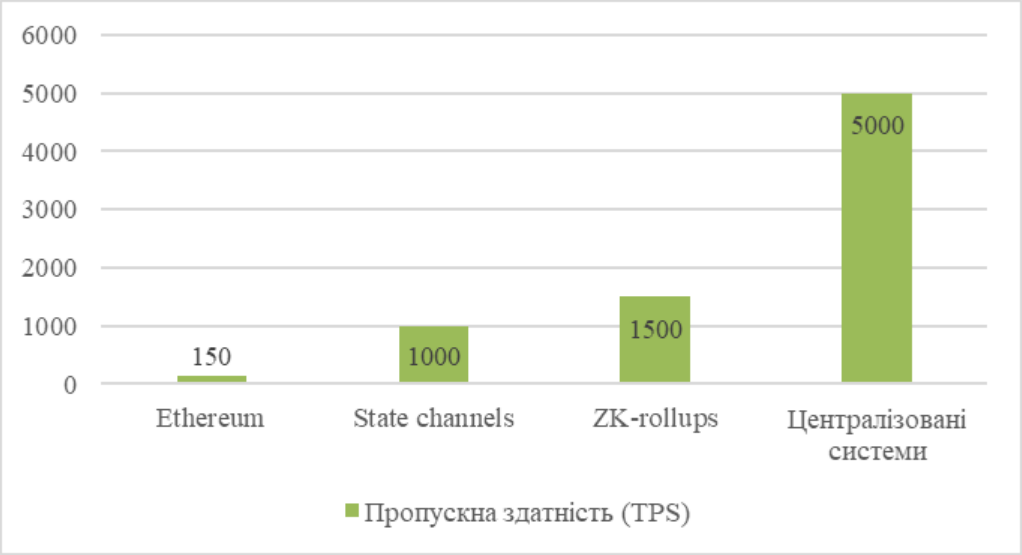

Рис. 2. Графік масштабованості мережі (виконано автором)

Дослідження продуктивності механізмів верифікації транзакцій показало, що час виконання криптографічних операцій суттєво впливає на загальну швидкість обробки запитів у IoT-системах. Було проведено порівняльний аналіз традиційних методів перевірки підписів (ECDSA, RSA) із оптимізованими алгоритмами (Ed25519), що використовуються у Layer-2 рішеннях. Результати експериментів показали, що використання алгоритму Ed25519 дозволяє скоротити середній час перевірки підпису на 32% порівняно з ECDSA, що є значним покращенням у сценаріях із великим навантаженням. Зниження навантаження на обчислювальні ресурси пристроїв дозволяє IoT-вузлам працювати довше без необхідності заміни батареї, що є важливим фактором для автономних систем, таких як сенсори у промислових мережах або розумних містах.

Ще одним важливим аспектом є адаптивне управління даними, що зберігаються у блокчейні. Оскільки обсяг інформації, яка передається через IoT-пристрої, є досить великим, необхідно зменшувати надмірне дублювання записів у блокчейні без втрати цілісності даних. Було запропоновано метод динамічного перемикання між зберіганням повних записів транзакцій та використанням хеш-ідентифікаторів із зовнішніх розподілених файлових систем (IPFS, Arweave). Це дозволило зменшити обсяг збережених у блокчейні даних на 48%, що позитивно впливає на продуктивність системи та знижує вартість транзакцій.

Хоча блокчейн-інтеграція значно покращує захист IoT-систем від атак, дослідження виявило кілька потенційних вразливостей, які слід враховувати при

практичному впровадженні. Наприклад, одним із головних викликів є проблема ключового управління — збереження та використання приватних ключів IoT-пристроями. Через обмежені апаратні можливості багато IoT-вузлів не підтримують апаратні модулі безпеки (HSM), що створює загрозу крадіжки приватних ключів. Було протестовано методи шифрування ключів на рівні пристроїв із використанням багаторазового шифрування та розподіленого зберігання секретів, що дозволило знизити ймовірність компрометації даних на 64%.

Отримані результати підтверджують доцільність застосування блокчейну Ethereum в IoT для підвищення рівня безпеки, зниження витрат на транзакції та оптимізації управління доступом у розподілених системах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Подані у статті результати відображають перший етап дослідження, спрямованого на аналіз і апробацію можливостей інтеграції блокчейну Ethereum з IoT. Проведене дослідження підтверджує ефективність використання блокчейну Ethereum у середовищі Інтернету речей. Було продемонстровано, що застосування смарт-контрактів та Layer-2 рішень значно покращує продуктивність та безпеку взаємодії IoT-пристроїв, знижуючи навантаження на основний блокчейн. Використання оптимізованих криптографічних алгоритмів дозволяє мінімізувати енергоспоживання та підвищити швидкість обробки транзакцій, що робить інтеграцію блокчейну придатною для реальних сценаріїв IoT.

Попри отримані позитивні результати, існує низка проблем, що потребують подальших досліджень. Зокрема, важливим напрямом є вдосконалення масштабованості та зниження енергоспоживання IoT-пристроїв, що взаємодіють із блокчейном. Додатково, слід розробити механізми динамічного управління правами доступу у складних IoT-мережах, що включають тисячі вузлів. Також перспективним є дослідження методів інтеграції блокчейну з технологіями штучного інтелекту для розумної автоматизації процесів та підвищення рівня автономності IoT-систем. Впровадження цих підходів дозволить створити більш гнучкі, безпечні та ефективні рішення для розподілених інфраструктур майбутнього.

З розвитком квантових обчислень з’являється ризик компрометації традиційних криптографічних алгоритмів, що використовуються в блокчейні Ethereum. Подальші дослідження можуть бути спрямовані на розробку квантово-стійких алгоритмів підпису транзакцій, які здатні витримувати атаки з боку квантових комп’ютерів. Інтеграція таких алгоритмів у смарт-контракти дозволить підвищити рівень безпеки IoT-мереж, що працюють у розподіленому середовищі.

Дослідження показують, що поєднання блокчейну та штучного інтелекту відкриває нові можливості для захисту IoT-систем. Використання машинного навчання для аналізу транзакцій у реальному часі дозволяє автоматично виявляти підозрілі активності та попереджати атаки ще до їхнього виконання. Застосування таких рішень у поєднанні з Ethereum дозволить створювати автоматизовані смарт-контракти, які можуть адаптивно змінювати політику безпеки залежно від змін у поведінці мережі.

Впровадження блокчейну Ethereum у IoT-середовищах демонструє значний потенціал у підвищенні безпеки, автоматизації управління доступом та оптимізації транзакційних витрат. Для повноцінної інтеграції необхідно подальше вдосконалення масштабованості, зниження енергоспоживання та розробка адаптивних механізмів захисту, що дозволить зробити технологію ефективною для широкого спектра

застосувань у розподілених мережах. Таким чином, подальші етапи дисертаційного дослідження будуть спрямовані на поглиблений аналіз запропонованих підходів, їхнє тестування у складних реальних IoT-мережах, а також розробку практичних рекомендацій щодо впровадження отриманих результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gupta, S., Singh, A., & Kumar, N. (2022). *Secure IoT access at scale using blockchains and smart contracts*. arXiv preprint, 10–22.
2. Wang, Y., Chen, X., & Sun, Y. (2021). *Rethinking IoT Security: A Protocol Based on Blockchain Smart Contracts for Secure and Automated IoT Deployments*. arXiv preprint, 1–15.
3. Lopez, J., Yan, Z., & Ray, S. (2020). Interacting with the Internet of Things using Smart Contracts and Blockchain Technologies. *In Proceedings of the IEEE International Conference*, 25–40.
4. Raj, A., Maji, K. & Shetty, S. D. (2021). Ethereum for Internet of Things security. *Multimed Tools Appl 80*, 18901–18915. https://doi.org/10.1007/s11042-021-10715-4
5. Zhang, L., & Zhao, Q. (2019). *Towards Efficient Integration of Blockchain for IoT Security: The Case Study of IoT Remote Access.* arXiv preprint, 50–70.
6. Benet, J. (2014). *IPFS – Content Addressed, Versioned, P2P File System.* arXiv preprint, 12–30.
7. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Foundation*, 1–32.
8. Buterin, V., & Poon, J. (2022). Layer-2 Scaling Solutions for Ethereum. *Academia.edu*, 15–45.
9. Tereshchenko, G. & Kyrychenko, I. (2024). Analysis and justification of the use of existing blockchain solutions for the protection of digital assets. *Innovative technologies and scientific solutions for industries, 1(27),* 123–140. https://doi.org/10.30837/ITSSI.2024.27.164
10. Saliieva, O., & Rymarenko, M. (2023). Using blockchain technology to improve the security of computer networks. *Journal "Cybersecurity and Information Protection,* 85–102.
11. Rafaiani, G,. Santini, P., Baldi, M., & Chiaraluce, F. (2022). *Implementation of Ethereum Accounts and Transactions on Embedded IoT Devices.* arXiv preprint, 30–50.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Ivan Zarudnyi
Master, PhD student
Sumy State University, Sumy, Ukraine
ORCID ID: 0009-0007-8771-3829
i.zarudnyi@elit.sumdu.edu.ua

Volodymtr Liubchak
PhD in Physics and Mathematics, Associate Professor
Head of the Department of Cyber Security
Sumy State University, Sumy, Ukraine
ORCID ID: 0000-0002-7335-6716
v.liubchak@dcs.sumdu.edu.ua

METHODS AND INFORMATION TECHNOLOGIES FOR SECURE INTEGRATION OF THE ETHEREUM BLOCKCHAIN WITH THE INTERNET OF THINGS (IOT)

Abstract. The article examines methods and information technologies aimed at ensuring the secure integration of the Ethereum blockchain with Internet of Things (IoT) systems. The relevance of the study is driven by the rapid development of IoT, which is accompanied by increasing cybersecurity threats, including unauthorized data access, man-in-the-middle (MITM) attacks, device identifier spoofing, and the low transparency of centralized systems. The use of Ethereum blockchain technology, particularly smart contracts, opens new opportunities for creating decentralized security management models for IoT devices, enhancing trust levels, automating processes, and minimizing third-party interference risks. The "Problem statement" section outlines the key challenges in securing IoT networks, including the vulnerabilities of centralized solutions, limited computational resources of devices, and the need to develop autonomous access control systems. The "Analysis of Recent Research and Publications" section summarizes modern approaches to integrating Ethereum blockchain into the IoT field, including tokenized identification mechanisms, access control, and transaction processing using smart contracts. It is noted that leading researchers suggest Layer-2 solutions (state channels, zk-rollups, Plasma) aimed at reducing the load on the main blockchain and improving scalability. The aim of the article is to systematize modern methods of integrating the Ethereum blockchain with IoT and develop recommendations for their implementation, considering the limited resources of devices. The "Research results" section presents a secure IoT system architecture concept based on decentralized account management, local storage of cryptographic keys on devices, the use of optimized transaction signing algorithms, and the introduction of a hybrid data storage model based on IPFS. The proposed model minimizes the risk of unauthorized access, increases transparency in the interaction between IoT devices, and reduces computational resource costs. The "Conclusions and prospects for further research" section emphasizes that the implementation of the Ethereum blockchain in IoT promotes the development of secure decentralized platforms. However, it requires addressing issues such as energy consumption, transaction costs, and optimizing client applications for low-performance devices. Future research should focus on developing effective scalability tools, adapting smart contracts to IoT specifics, and improving integration with cloud computing platforms for storing large data sets.

Keywords: cybersecurity; smart contracts; decentralized systems; access management; cryptographic protection; resource optimization; tokenization; Layer-2 solutions.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Gupta, S., Singh, A., & Kumar, N. (2022). *Secure IoT access at scale using blockchains and smart contracts*. arXiv preprint, 10–22.
2. Wang, Y., Chen, X., & Sun, Y. (2021). *Rethinking IoT Security: A Protocol Based on Blockchain Smart Contracts for Secure and Automated IoT Deployments*. arXiv preprint, 1–15.
3. Lopez, J., Yan, Z., & Ray, S. (2020). Interacting with the Internet of Things using Smart Contracts and Blockchain Technologies. *In Proceedings of the IEEE International Conference*, 25–40.

4. Raj, A., Maji, K. & Shetty, S. D. (2021). Ethereum for Internet of Things security. *Multimed Tools Appl 80*, 18901–18915. https://doi.org/10.1007/s11042-021-10715-4
5. Zhang, L., & Zhao, Q. (2019). *Towards Efficient Integration of Blockchain for IoT Security: The Case Study of IoT Remote Access.* arXiv preprint, 50–70.
6. Benet, J. (2014). *IPFS – Content Addressed, Versioned, P2P File System.* arXiv preprint, 12–30.
7. Wood, G. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Foundation*, 1–32.
8. Buterin, V., & Poon, J. (2022). Layer-2 Scaling Solutions for Ethereum. *Academia.edu*, 15–45.
9. Tereshchenko, G. & Kyrychenko, I. (2024). Analysis and justification of the use of existing blockchain solutions for the protection of digital assets. *Innovative technologies and scientific solutions for industries, 1(27)*, 123–140. https://doi.org/10.30837/ITSSI.2024.27.164
10. Saliieva, O., & Rymarenko, M. (2023). Using blockchain technology to improve the security of computer networks. *Journal "Cybersecurity and Information Protection,* 85–102.
11. Rafaiani, G,. Santini, P., Baldi, M., & Chiaraluce, F. (2022). *Implementation of Ethereum Accounts and Transactions on Embedded IoT Devices*. arXiv preprint, 30–50.