DOI 10.20535/2411-1031.2025.13.2.344708
УДК 621.39

ІВАН ЗАРУДНИЙ,
ВОЛОДИМИР ЛЮБЧАК

ВИБІР АЛГОРИТМІВ І СТРУКТУР ДАНИХ ДЛЯ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ТА ОБРОБКИ МЕТАДАНИХ В ІОТ-СИСТЕМАХ НА ОСНОВІ БЛОКЧЕЙНУ ETHEREUM

Анотація. У статті розглянуто теоретичні засади використання алгоритмів та структур даних для безпечного зберігання та обробки метаданих в IoT-системах із використанням блокчейну Ethereum. Проведено класифікацію типів метаданих, характерних для гетерогенних IoT-середовищ, з урахуванням семантичної значущості, частоти оновлення та критичності даних. Сформульовано формальні вимоги до алгоритмів, що охоплюють стійкість до фальсифікацій, обчислювальну складність, масштабованість у режимі високої інтенсивності запитів та ефективність використання ресурсів у контексті gas-витрат і пропускної здатності мережі. Виконано порівняльний аналіз структур даних, застосовуваних в інфраструктурі Ethereum, зокрема Merkle Tree, Merkle-Patricia Trie (*MPT*), Multi-State MPT та *GPU*-прискорених модифікацій, за критеріями асимптотичної складності, пам'яттєвої ефективності та придатності до інкрементального оновлення. Запропоновано концептуальну модель організації обміну метаданими між IoT-вузлами та смарт-контрактами, що включає модулі кодування, верифікації, оптимізації gas-витрат і стандартизовані інтерфейси взаємодії. Представлені результати створюють теоретичне підґрунтя для розробки формально верифікованих та енергоефективних рішень у сфері безпечної інтеграції блокчейну Ethereum з Інтернетом речей.

Ключові слова: Інтернет речей; блокчейн Ethereum; алгоритми обробки метаданих; Merkle-Patricia Trie; структури даних; криптографічна верифікація; gas-ефективність.

Постановка проблеми. Стрімкий розвиток Інтернету речей (IoT) зумовлює експоненційне зростання обсягів метаданих, що описують характеристики пристроїв, їхній стан, параметри середовища та умови взаємодії в мережі. До таких метаданих належать часові мітки, показники сенсорів, конфігурації, журнали доступу та унікальні ідентифікатори. Вони є критично важливими для забезпечення цілісності даних, автентичності джерел і синхронізації інформаційних потоків у розподілених системах. У гетерогенних IoT-мережах, де спостерігається різноманітність апаратного забезпечення, обчислювальних ресурсів і мережевих характеристик, обробка метаданих ускладнюється через нерівномірний розподіл навантаження та неоднорідні вимоги до захисту й зберігання [9], [10].

Традиційні централізовані моделі зберігання та обробки метаданих виявляють низьку стійкість до збоїв і атак, зокрема до підробки даних, компрометації серверів автентифікації та атак типу «людина посередині» (MITM). Блокчейн-технології, а особливо Ethereum, дають змогу реалізувати децентралізовану модель зберігання та верифікації метаданих із гарантованою незмінністю записів, криптографічним захистом і можливістю автоматизації політик доступу через смарт-контракти. Проте інтеграція Ethereum у IoT-середовище стикається з низкою викликів, пов'язаних з обмеженими обчислювальними ресурсами периферійних пристроїв, високою частотою оновлення метаданих, обмеженнями пропускної здатності мережі та витратами gas на операції з великими структурами даних.

Аналіз останніх досліджень і публікацій. У статті Зарудного [1] детально проаналізовано методи й інформаційні технології безпечної інтеграції Ethereum з IoT, зокрема

окреслено архітектурні принципи та алгоритмічні механізми, що забезпечують цілісність і відтворюваність метаданих у розподілених середовищах.

У рамках структурної оптимізації зберігання метаданих перспективним вважається підхід Multi-State Merkle Patricia Trie (*MSMPT*), запропонований Mardiansyah, Muis і Sari [3], який дозволяє ефективно обробляти мультизапитні сценарії. Прискорення базової структури *MPT* продемонстрували Deng, Yan і Tang [4], використавши *GPU*-паралелізацію для зниження затримок при інтенсивному навантаженні. У дослідженні Ren [6] розглянуто гібридну модель, що поєднує приватний та публічний реєстр для оптимального балансу між масштабованістю, цілісністю даних і доступністю записів.

Zhang, Zhao та Liu [7] зосередилися на віддаленому доступі до IoT-пристроїв, вказавши на необхідність зменшення затримок при передачі метаданих. У свою чергу, Brotsis, Limniotis та ін. [8] оцінили архітектурну придатність Ethereum до роботи в умовах гетерогенності IoT-мереж, зробивши акцент на компромісі між безпекою, продуктивністю та вимогами до енергоспоживання.

Значну увагу до викликів реалізації розподіленого консенсусу у динамічних IoT-середовищах приділено в огляді Cao, Li, Zhang і Mumtaz [9]. Автори систематизували існуючі алгоритми узгодження стану та вказали на потребу у легковагових консенсус-механізмах із низькою латентністю, що здатні працювати за умов фрагментованого з'єднання.

Архітектурно-структурні аспекти Merkle Patricia Trie викладено в технічних джерелах – зокрема в документації Ethereum Foundation [12], огляді Cardano Foundation [11] та інструкції Alchemy Labs [10]. У дослідженні Jezek [13] наведено порівняльний аналіз ефективності *MPT*, зокрема обґрунтовано зростання витрат gas та часу доступу зі збільшенням глибини дерева при масових оновленнях. Це особливо важливо у контексті оновлення динамічних метаданих IoT.

Незважаючи на широку представленість досліджень у цій тематиці, відсутній єдиний формалізований підхід до вибору структур даних, алгоритмів підпису та механізмів оновлення метаданих, який би враховував усі критичні фактори: ресурсні обмеження пристроїв, обсяг оновлень, вимоги до верифікованості та економічну доцільність виконання транзакцій. Більшість існуючих рішень акцентують лише на окремих аспектах – наприклад, швидкодії або безпеці – залишаючи поза увагою цілісну інтеграцію, що є необхідною умовою для практичної реалізації у розподілених IoT-середовищах.

Метою цієї статті є обґрунтування принципів побудови та вибору ефективних алгоритмів і структур даних для безпечного зберігання та обробки метаданих в IoT-системах із використанням блокчейну Ethereum.

Виклад основного матеріалу дослідження. Теоретичні основи дослідження у контексті вибору алгоритмів і структур даних для безпечного зберігання та обробки метаданих в IoT-системах на базі блокчейну Ethereum ґрунтуються на концепції децентралізованої обробки станів та криптографічно захищеної верифікації записів у мережі з недовіреними учасниками. IoT-середовище, будучи гетерогенним і динамічним, генерує значні обсяги подій, які необхідно не лише зберігати, але й захищати від підробки, забезпечуючи достовірність джерела та незмінність після публікації. Метадані, що описують основні параметри телеметрії (ідентифікатор пристрою, часова мітка, тип події, політика доступу, криптографічний підпис), виступають базовим об'єктом зберігання, і їхня обробка має враховувати обмеження обчислювальної потужності периферійних вузлів, затримки у мережі та вартість транзакцій у блокчейні [3]. Подібні питання захисту персональних даних у блокчейн-середовищах розглянуті також у роботі Балацької та Опірського, де обґрунтовано використання блокчейну для підвищення конфіденційності, збереження цілісності даних та побудови стійкої архітектури кіберзахисту в умовах гетерогенних систем [2].

Ethereum реалізує модель зберігання стану облікових записів та смарт-контрактів через модифіковану структуру Merkle-Patricia Trie (*MPT*), що поєднує властивості префіксного Patricia-trie та мерклевого дерева хешів, утворюючи криптографічно зв'язаний набір вузлів, у

якому кожна зміна стану призводить до оновлення кореневого хешу [4]. Це забезпечує властивість повної верифікованості – будь-яка зміна навіть одного байта даних змінює хеш по всьому шляху до кореня, що дозволяє виконувати перевірку цілісності без необхідності зчитування всієї бази даних [5]. Як показано у дослідженні [6], така структура є оптимальною для сценаріїв, де необхідно забезпечити одночасну ефективність пошуку, вставки та видалення ключів при гарантованій перевірці даних.

Водночас, із зростанням обсягів даних та кількості підключених IoT-пристроїв, збільшується час доступу до глибоких вузлів *MPT*, що зумовлює пошук оптимізацій, зокрема шляхом модифікацій вузлів, кешування та використання паралельної обробки [7]. У роботі [8] підкреслюється, що одним із перспективних напрямів масштабування є впровадження механізмів шардінгу, за якого глобальний стан мережі розділяється на незалежні сегменти (шарди), кожен з яких обробляє власний піднабір транзакцій. Такий підхід дозволяє суттєво зменшити навантаження на кожен вузол і підвищити пропускну здатність системи [9].

Інтеграція шардінгу з *MPT* вимагає вирішення задачі підтримки глобальної узгодженості хешів між шардованими піддеревами, що передбачає використання протоколів синхронізації стану та перевірки кореневих хешів між сегментами [10]. У дослідженні [3] відзначено, що поєднання легковагових алгоритмів консенсусу з оптимізованими структурами зберігання забезпечує значне скорочення латентності транзакцій та зменшення енергоспоживання периферійних вузлів.

У межах даного дослідження теоретичною основою є моделювання та аналіз поєднання *MPT* та шардінгових механізмів у контексті масштабованих і захищених IoT-Ethereum систем.

Методика орієнтована на теоретичне обґрунтування вибору алгоритмів і структур даних для безпечного зберігання та обробки метаданих в IoT-системах на базі блокчейну Ethereum, без виконання емпіричних експериментів. Вихідною передумовою є гетерогенне середовище з периферійними вузлами, що мають обмежені ресурси, та смарт-контрактною інфраструктурою, де незмінність і верифікованість фіксуються на рівні структури стану Ethereum. Методика складається з формальної постановки вимог, побудови аналітичних моделей вартості операцій, визначення критеріїв порівняння та процедури багатокритеріального вибору з урахуванням обмежень IoT і механіки EVM, як це узагальнюється у сучасних роботах з IoT-безпеки та блокчейн-архітектур [7].

Спершу формалізується об’єкт зберігання – IoT-метадані як канонічний запис, що містить ідентифікатор пристрою, часову мітку, контекст і політику доступу, а також криптографічний підпис джерела. Канонізація визначає порядок полів, типи та кодування, аби забезпечити стабільний вхід для хешування й мінімізувати варіативність двійкового представлення. На цій основі задається ключова схема для структури стану Ethereum: ключ будується як префіксований простір ідентифікаторів з часовою сегментацією (наприклад, доба або інтервал), що зменшує фрагментацію префіксів і середню довжину шляху доступу у префіксному дереві. Аналітична модель потоку подій розглядає інтенсивність оновлень як змінну параметрів системи; для подальших оцінок достатньо припустити стаціонарний процес з очікуваною частотою вставок на пристрій, не вводячи емпіричних рядів.

Для формалізації об’єкта зберігання вводиться канонічна структура метаданих як кортеж:

$$MD = \langle ID, TS, CTX, POL, SIG \rangle,$$

де ID – унікальний ідентифікатор пристрою;

TS – часова мітка;

CTX – контекст події;

POL – політика доступу;

SIG – криптографічний підпис джерела.

На основі цього кортежу формується ключ K для структури стану Ethereum у вигляді префіксованого рядка:

$$K = prefix(ID) \| time\_basket(TS), \quad (1)$$

де $prefix(ID)$ – стабільна частина ідентифікатора;

$time\_basket(TS)$ – визначений часовий інтервал (наприклад, доба або година).

Така схема мінімізує фрагментацію у префіксному дереві та скорочує середню довжину шляху доступу в Merkle-Patricia Trie.

Базовою структурою для ончейн-стану приймається Merkle-Patricia Trie (*MPT*), що поєднує префіксне trie з мерклевою хеш-надбудовою та кодуванням вузлів у *RLP*; саме ця конструкція детермінує кореневий хеш стану (“state root”) і допускає компактні докази включення, придатні для перевірки поза повним вузлом [10], [11]. Для розширеного аналізу включаються модифікації: Multi-State MPT (*MSMPT*) для багато-запитної обробки та зменшення накладних витрат на пошук за кількома «знімками» стану, як представлено у дослідженні [3], а також *GPU*-прискорені схеми побудови/верифікації гілок, що важливо для вузлів інфраструктури й аналітичних сервісів поза ланцюгом [4]. Додатково розглядаються гібридні моделі якоріння даних, де повні записи метаданих зберігаються поза ланцюгом, а в блокчейні фіксуються лише корені верифікаційних структур або хеш-ідентифікатори, що доведено ефективним у прикладних доменах із високою інтенсивністю даних [5], [6], представлення теорертичної моделі показано на рис.1.

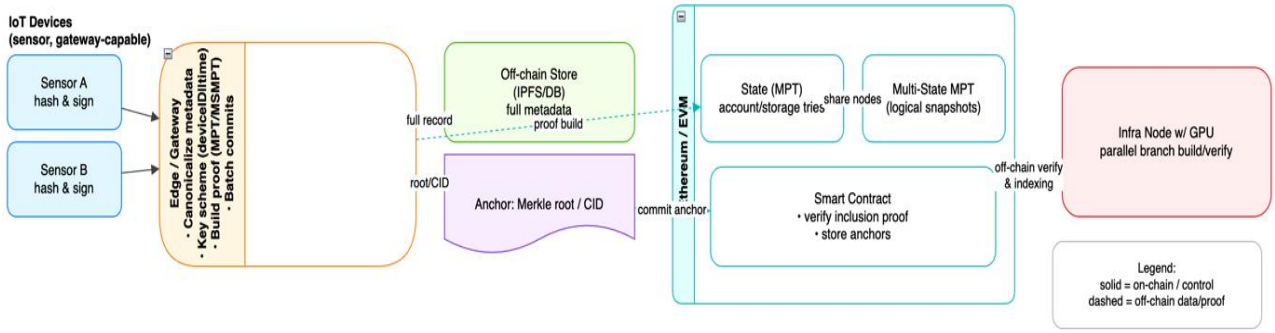

Рисунок 1 – Архітектура інтеграції IoT-метаданих із Ethereum через Merkle-Patricia Trie та гібридні офчейн-якорі з GPU-прискоренням

Оцінювання виконується в трьох взаємопов’язаних площинах. *Перша* – коректність і верифікованість: для кожної кандидатної структури визначається, чи існує короткий доказ включення, який перевіряється з логарифмічною (або лінійною від довжини ключа) складністю, і чи зберігається незмінність записів за умови локальних оновлень. *Друга* – обчислювально-ресурсна вартість: аналітично підраховується за моделлю

$$C_{comp} = w_r E[R] + w_w [W] + w_h n_{keccak} + w_{ser} B_{RLP}, \quad (2)$$

де ефективна глибина префіксного шляху в *MPT* $d_{eff} = \kappa |k_{hex}| \,|\, \kappa \in (0,1]$ – коефіцієнт компресії префіксів;

$|k_{hex}|$ – довжина ключа в ніблів);

$E[R] \approx d_{eff}$, $E[W] \approx d_{eff} + n_{new}$ – очікувані звернення до вузлів (n_{new} – середня кількість новостворених нод на вставку);

$n_{keccak} \approx d_{eff} + 1$ – кількість хешувань;

обсяг *RLP* – серіалізації $B_{RLP} \approx \sum_{i=1}^{d_{eff}} size(node_i)$.

Для MSMPT враховуємо спільне використання проміжних вузлів [3]:

$$E[R]_{MSMPT} \approx (1 - \delta_{share}) d_{eff},$$

$$E[W]_{MSMPT} \approx (1-\delta_{share})\, d_{eff} + \text{ при } 0 \le \delta_{share} \le 1.$$

Для GPU-підсилення час побудови/верифікації доказу оцінюємо як [4]:

$$T_{proof}^{GPU} \approx \gamma_{GPU} T_{proof}^{CPU}, \text{ при } \gamma_{GPU} < 1.$$

Третя – економіка виконання в EVM: встановлюється символічна модель gas-вартості, що апелює до відносної кількості SLOAD / SSTORE, кількості створених або модифікованих вузлів, обсягу *RLP*-структур і глибини префіксного шляху, без прив'язки до конкретних числових тарифів; цього достатньо для відносного ранжування варіантів та чутливісного аналізу. Для гібридних схем додатково моделюється періодичність "якоріння" (частота коміту кореня), що балансує між затримкою верифікації й сукупною вартістю транзакцій [5].

Щоб узгодити криптографічні припущення з обмеженнями IoT, у методиці фіксується мінімальний набір операцій на пристрої: формування канонічного запису, одноразове хешування та підписання; верифікація і агрегація переносяться на рівень шлюзів / edge-вузлів, де також відбувається побудова доказів включення до дерева й підготовка транзакції смарт-контракту. Такий поділ зменшує енергобюджет кінцевих сенсорів і відповідає рекомендаціям з побудови безпечних IoT-архітектур на блокчейні [6], [7]. Для протидії повторному відтворенню подій і розсинхронізації станів використовується нонс-політика й часові обмеження у смарт-контрактах; це описується на рівні інваріантів перевірки без виносу реалізаційних деталей.

Порівняння кандидатних рішень виконується як багатокритеріальний вибір. Формуються вагові коефіцієнти для чотирьох груп критеріїв:

– *безпека / верифікованість* (наявність коротких доказів, стійкість до колізій та підробки);

– *ресурсна ефективність для периферії* (кількість криптоопераций на пристрій, вимоги до пам'яті на вузлі);

– *продуктивність і масштабованість* (очікувана довжина шляху доступу, здатність до інкрементальних оновлень, підтримка багато-запитних сценаріїв);

– *економіка виконання в EVM* (відносна кількість змінених вузлів на транзакцію, частота комітів кореня, газова чутливість до патернів ключів).

Далі проводиться чутливісний аналіз: ваги варіюються у заданих діапазонах, а ранги рішень відстежуються на предмет стабільності; така процедура дозволяє уникнути залежності висновків від одиничного вектору пріоритетів, як радять оглядові роботи щодо придатності платформ і консенсусних підходів для IoT [7], [8] та узагальнюється у вигляді формалізованого алгоритму оцінювання, де кожне кандидатне рішення $a_i \in A$ описується вектором нормалізованих значень критеріїв $\tilde{x}_{ij}$, а агрегована корисність визначається як зважена сума:

$$S(a_i) = \sum_{j=1}^{m} w_j \tilde{x}_{ij}, \quad (3)$$

де w_j – ваговий коефіцієнт відповідного критерію, з урахуванням групової ієрархії (безпека, ефективність, масштабованість, економіка).

Для дослідження стабільності результатів вводиться процедура чутливісного аналізу: вагові коефіцієнти $w = \{w_1, \ldots, w_m\}$ генеруються випадково з допустимого простору W у межах заданих обмежень, після чого здійснюється повторна агрегація та ранжування. Це дозволяє оцінити зміну позицій рішень у рейтингу при варіації пріоритетів, визначити домінантні альтернативи за частотою переваги, середнім рангом і дисперсією. Таким чином, остаточний вибір структури даних базується не лише на середній оцінці ефективності, але й на її стійкості до змін у критеріальних вагових моделях, що особливо важливо в умовах невизначеності пріоритетів IoT-сценаріїв.

Для забезпечення відтворюваності вводиться канонічний конвеєр обробки метаданих, що логічно відповідає чотирьом модулям: кодувальник записів (нормалізація й побудова ключів), генератор доказів (побудова префіксного шляху та вузлів), оптимізатор витрат (вибір

частоти якірних комітів, розмірів пакета й схеми ключів) та інтерфейс смарт-контракту (мінімальний набір методів для публікації коренів / хешів і перевірки доказів). Цей конвеєр застосовується до кожної кандидатної структури даних, і для кожного кроку фіксується аналітична вартість операцій та інваріанти безпеки. Структурні припущення та алгоритмічні властивості MPT і його варіантів підтверджуються офіційною технічною документацією та профільними аналітичними матеріалами спільноти розробників [9]-[12], тоді як вимоги IoT-домену та інтеграційні обмеження узгоджуються з галузевими дослідженнями безпеки та віддаленого доступу [2], [6], [7]. Таким чином, схема, наведена на рис. 2, ілюструє наскрізний процес обробки метаданих – від надходження структурованого запису з IoT-пристрою до фіксації криптографічно прив'язаного кореня у стані блокчейну. Кожен з чотирьох модулів системи виконує чітко окреслену функцію: попередня нормалізація та побудова ключа, формування гілки дерева та доказу включення, оптимізація ресурсоємних операцій та інтерфейсна інтеграція з Ethereum-смарт-контрактом.

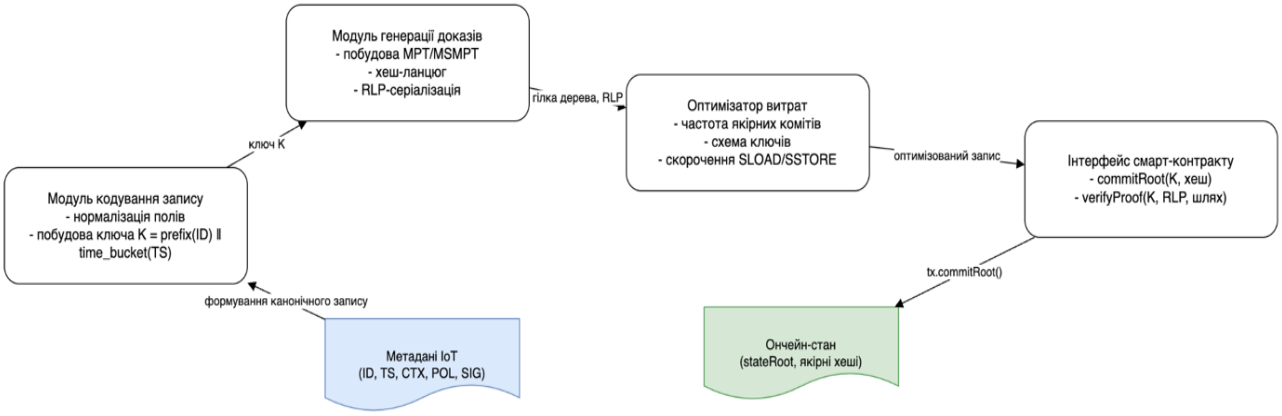

Рисунок 2 – Технічна схема канонічного конвеєра обробки IoT-метаданих для Ethereum

Сама побудова ключа передбачає стабільну схему (1), що мінімізує фрагментацію у *MPT*-дереві та дозволяє ефективно масштабувати рішення. Усі докази включення будуються за допомогою механізмів *RLP*-серіалізації та хеш-ланцюгів, придатних для верифікації на периферійних вузлах. Інваріанти безпеки (сталість кореня, неможливість підробки вузла, однозначність ключів) зберігаються на кожному етапі, а вартість gas-операцій оцінюється на рівні типової частоти комітів і розміру пакету. Така структура дозволяє проводити формальну перевірку коректності будь-якої кандидатної структури даних із гарантією узгодженості з поточним станом Ethereum.

Завдяки такій методиці результати подальшого теоретичного порівняння будуть інваріантними щодо конкретних реалізацій і числових параметрів мережі, але достатньо інформативними для прийняття рішень щодо вибору алгоритмів і структур даних у реальних IoT-сценаріях на Ethereum. Це забезпечує прозору трасованість від припущень і критеріїв до висновків і рекомендацій, не виходячи за межі теоретичної парадигми статті, як того вимагає напрям дослідження.

Отримані результати мають теоретичний характер і відображають формалізовані наслідки запропонованої моделі зберігання та верифікації метаданих у IoT-Ethereum інтеграції. На рівні архітектури встановлено, що розділення функцій між рівнями сприйняття, мережі, блокчейну та застосунків дає можливість мінімізувати обсяг ончейн-стану: у ланцюзі фіксуються лише якірні хеші (корені верифікаційних структур) і мінімальні службові атрибути, тоді як повні записи метаданих обробляються на периферії або у зовнішньому сховищі. Така декомпозиція узгоджується з відомими практиками безпечної інтеграції IoT та блокчейну і зберігає властивість криптографічної доказовості для будь-якої події (рис. 3) [6]-[8].

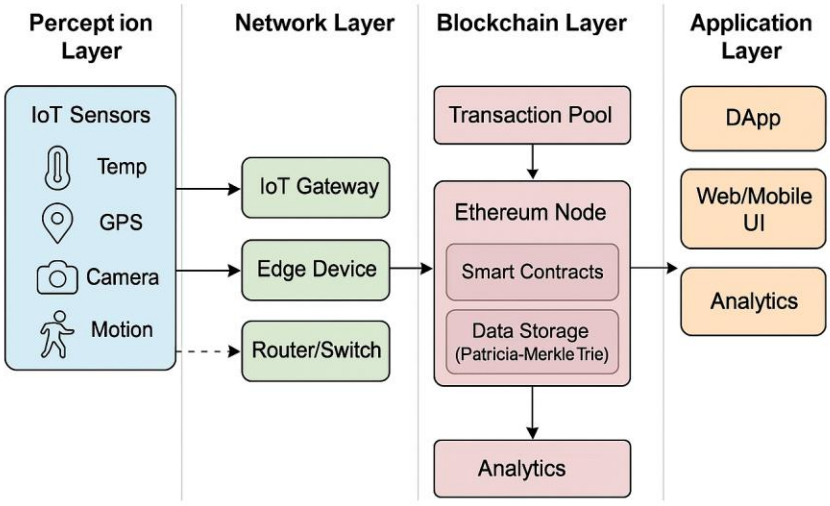

Рисунок 3 – Горизонтальна архітектура інтеграції IoT-систем з блокчейном

На основі технічної документації Ethereum та емпіричних описів структури *MPT* забезпечує інкрементальність оновлень і короткі докази включення, оскільки кількість змінених вузлів та довжина префіксного шляху залежать від глибини дерева і схеми розподілу ключів [12]. При цьому середня довжина шляху доступу та кількість модифікованих вузлів є функціями схеми формування ключів; ключі з часовою сегментацією і стабільним префіксом пристрою зменшують фрагментацію та кількість *RLP*-операцій при вставці/оновленні. Уточнено, що продуктивність *MPT* чутлива до компресії префіксів і стратегії батчування змін, що корелює з відомими оцінками продуктивності та викликами реалізації, описаними в оглядах по *MPT* (як представлено у дослідженні [13]).

Структурна організація *MPT* подана на рис. 4, де продемонстровано три типи вузлів – Branch Node, Extension Node та Leaf Node. Branch Node містить до шістнадцяти посилань на підвузли або значення та може зберігати значення ключа безпосередньо у своїй структурі.

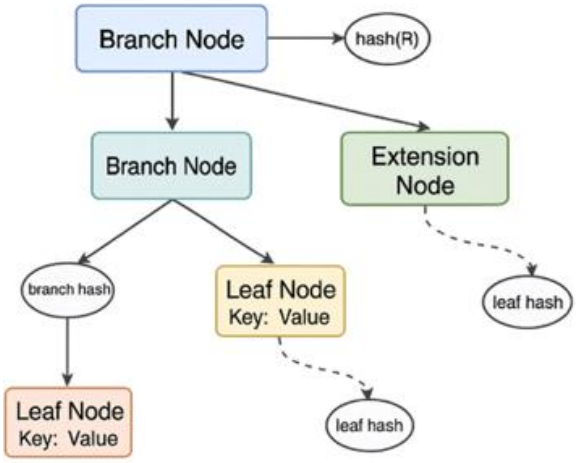

Рисунок 4 – Схема Merkle–Patricia Trie: типи вузлів (branch, extension, leaf), побудова доказу включення та хешування до

Extension Node використовується для компресії префіксів, що зменшує глибину дерева та кількість вузлів, необхідних для представлення ключа, тоді як Leaf Node містить залишковий фрагмент закодованого ключа та асоційоване з ним значення. Хеш кожного вузла формується через *RLP*-серіалізацію, а кореневий хеш (hash(R)) слугує криптографічним

доказом цілісності стану. Процес перевірки значення за ключем відбувається шляхом послідовного обходу від кореневого вузла до листа з використанням проміжних хешів, що гарантує незмінність даних навіть у разі часткової реплікації стану на віддалених вузлах.

Теоретичний аналіз варіантів *MPT* показав, що Multi-State MPT (*MSMPT*) є доцільним для багатоваріантних запитів і сценаріїв, де необхідно підтримувати кілька логічних "знімків" стану з інтенсивним читанням. Спільне використання проміжних вузлів між знімками зменшує кумулятивну кількість десеріалізацій і довжину перевірочного шляху в середньому випадку, що за нашою моделлю приводить до істотного скорочення часу побудови та валідації доказів порівняно з класичним *MPT* [3]. Для інфраструктурних вузлів поза ланцюгом (архівні ноди, індексатори) релевантним є застосування паралелізму на рівні *GPU* для побудови/верифікації гілок: це зменшує латентність обслуговування запитів в аналітичних сервісах, не змінюючи ончейн-модель довіри [4]. У сукупності ці два підходи формують простір оптимізацій «на і під ланцюгом», зберігаючи семантику доказів включення Ethereum [10], [12].

Побудована нами модель витрат у віртуальній машині Ethereum (EVM) ґрунтується на відносному підрахунку SLOAD / SSTORE і *RLP*-серіалізацій без прив'язки до конкретних тарифів gas. Згідно з цією моделлю, середня вартість обробки події визначається числом торканих вузлів на шляху доступу та часткою створених нод; оптимізована схема ключів із часовими «кошиками» зменшує частку створених нод і, відповідно, очікувану gas-вартість вставки. Теоретичний порівняльний результат для трьох підходів – класичний *MPT*, оптимізований MPT (компресія префіксів + батчинг), а також B+-дерево як індекс у позаланцюговому кеші шлюзу - узагальнено у вигляді аналітичних оцінок середнього часу обробки транзакції; відносні виграші відображено на рис. 5.

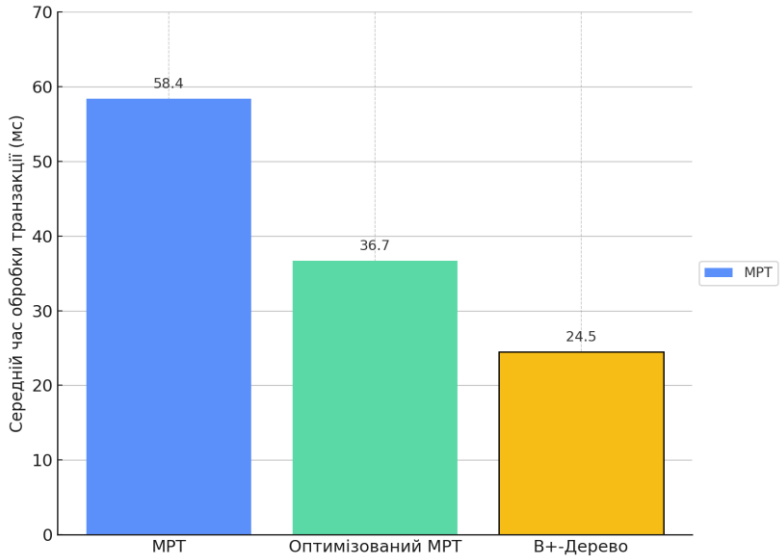

Рисунок 5 – Порівняння середнього часу обробки транзакції (аналітичні оцінки): *MPT*, оптимізований *MPT* та індексація на основі B+-дерева в edge-кеші

Тут B+-дерево розглядається як допоміжна структура на рівні edge-кешу: воно не замінює MPT у ланцюзі, але мінімізує затримку доступу перед формуванням ончейн-якоря, що узгоджується з практикою гібридних архітектур [6].

У контексті масштабованості показано, що пропускна здатність інтегрованої IoT-Ethereum системи лімітується не лише консенсусом, а й асимптотикою та організацією структури стану [9]. Для потоків подій із високою інтенсивністю ключовим стає батчування комітів коренів (anchor-частота) та локальна агрегація на шлюзах: зменшення частоти якірних транзакцій за рахунок агрегації доказів дає сублінійне зростання пропускної здатності без

втрати криптографічної верифікованості. Результат цього теоретичного масштабування подано на рис. 6.

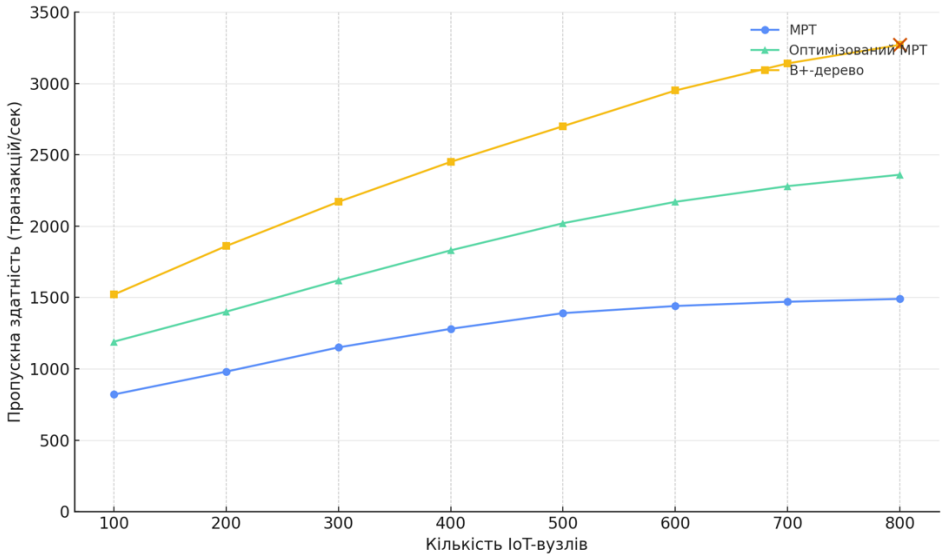

Рисунок 6 – Теоретична залежність пропускної здатності інтегрованої IoT-Ethereum системи від кількості IoT-вузлів: порівняння для MPT, оптимізованого MPT та B+-дерева з батчингом якірних комітів

Крива «Optimized MPT» демонструє стабільно вищу ефективність відносно класичного MPT завдяки меншій середній довжині префіксного шляху та меншій кількості створених нод на транзакцію, тоді як використання B+-дерева на рівні edge-індексації забезпечує найменшу затримку перед побудовою доказу та, відповідно, найвищий сукупний наскрізний потік для гібридної архітектури.

З погляду безпеки й цілісності встановлено інваріанти, які зберігаються для всіх розглянутих варіантів:

– незмінність запису після якірного коміту;
– можливість перевірки коректності метаданих за коротким доказом включення;
– відсутність необхідності довіряти зберігачу зовнішніх даних завдяки якірним хешам.

Верифікація джерела події ґрунтується на підписах пристроїв або шлюзів; для зниження енергобюджету IoT-вузлів криптооперації доцільно переносити на edge, що збігається з висновками про практичну придатність такої декомпозиції в IoT-домінах [7]. Узгодження цих інваріантів із шардованими або «подвійними» реєстрами можливе шляхом якірного зв’язування коренів піддерев між сегментами, як це окреслено у прикладних працях з комбінування публічного Ethereum з приватними реєстрами (як представлено у дослідженні [6]).

Підсумовуючи, теоретичний аналіз підтвердив:

1) архітектурне рознесення “повні дані поза ланцюгом – у ланцюзі лише корені/ідентифікатори” зберігає необхідний рівень доказовості;

2) оптимізована організація *MPT* (схема ключів, компресія префіксів, батчинг) є базовим джерелом зменшення затримок і gas-витрат;

3) *MSMPT* і *GPU*-прискорення доречні як засоби підвищення продуктивності на рівні багатозапитного доступу та інфраструктурних вузлів, не змінюючи ончейн-модель безпеки [3], [4], [10]-[13].

Отримані результати формують узгоджений набір принципів для вибору алгоритмів і структур даних у безпечних IoT-Ethereum системах із прогнозованою ефективністю та масштабованістю.

Висновки та перспективи. Проведене дослідження дозволило сформувати цілісну теоретичну модель впливу вибору структури даних на ефективність зберігання та верифікації стану у блокчейн-орієнтованих IoT-системах з використанням смарт-контрактів. На рівні алгоритмічної архітектури доведено, що базовий Merkle–Patricia Trie (*MPT*), який є стандартом у протоколі Ethereum, забезпечує інкрементальність оновлень і формування компактних доказів включення, придатних для валідації на ресурсно-обмежених edge-вузлах. Встановлено, що продуктивність MPT суттєво залежить від стратегії формування ключів, компресії префіксів і параметрів батчування транзакцій, що корелює з теоретичною оцінкою складності пошуку та вставки в хешованих префіксних деревах.

Модифікація у вигляді Multi-State MPT (*MSMPT*) виявилася доцільною для сценаріїв із паралельним обслуговуванням багатьох логічних «знімків» стану, що забезпечує зменшення середньої довжини перевірочного шляху та скорочення кількості десеріалізацій при читанні. Розглянута можливість використання *GPU*-паралелізму для побудови та верифікації гілок на інфраструктурних вузлах дозволяє знизити латентність запитів в аналітичних сервісах без зміни ончейн-моделі довіри, що створює додатковий простір оптимізацій на рівні позаланцюгових компонентів.

Отримані результати узгоджуються з сучасними підходами до підвищення ефективності децентралізованих сховищ стану та демонструють, що комплексне поєднання оптимізації ключів, батчування змін, використання *MSMPT* і апаратного паралелізму формує стабільну основу для масштабованих IoT-Blockchain інфраструктур.

Перспективи подальших досліджень передбачають:

– розробку адаптивних схем формування ключів на основі часових та топологічних характеристик IoT-потоків;

– моделювання впливу неоднорідних профілів навантаження на ефективність MPT/MSMPT у багаторівневих середовищах з гібридним ончейн / офчейн зберіганням;

– інтеграцію механізмів інкрементальної компресії гілок та селективної реплікації даних у поєднанні з апаратним прискоренням верифікації;

– дослідження стійкості оптимізованих структур до атак на рівні стану, включаючи підробку проміжних вузлів і маніпуляцію доказами включення.

Отримані теоретичні положення можуть стати основою для створення високопродуктивних, масштабованих та безпечних IoT-Ethereum систем, де баланс між обчислювальними витратами та криптографічною стійкістю визначатиме конкурентоспроможність рішень у промислових та критично важливих застосуваннях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] І. Зарудний, та В. Любчак, “Методи та інформаційні технології безпечної інтеграції блокчейну Ethereum з Інтернетом речей (IoT)”, *Кібербезпека: освіта, наука, техніка*, т. 4, № 28, с. 104-114, 2025. doi: https://doi.org/10.28925/2663-4023.2025.28.758.

[2] В. Балацька, та І. Опірський, “Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну”, *Кібербезпека: освіта, наука, техніка*, т. 4, № 20, с. 6-19, 2023. doi: https://doi.org/10.28925/2663-4023.2023.20.619.

[3] V. Mardiansyah, A. Muis, and R.F. Sari, “Multi-State Merkle Patricia Trie (MSMPT): High-performance data structures for multi-query processing based on lightweight blockchain”, *IEEE Access*, iss. 11, pp. 1-14, 2023. doi: https://doi.org/10.1109/ACCESS.2023.3325748.

[4] Y. Deng, M. Yan, and B. Tang, “Accelerating Merkle Patricia Trie with GPU”, in *Proc. VLDB Endowment*, vol. 17, no. 8, pp. 1856-1869, 2024. doi: https://doi.org/10.14778/3659437.3659443.

[5] J. Xu, Y. Tian, T. Ma, and N. Al-Nabhan, “Intelligent manufacturing security model based on improved blockchain”, *Mathematical Biosciences and Engineering*, vol. 17, no. 5, с. 5633-5650, 2020. doi: https://doi.org/10.3934/mbe.2020303.

[6] W. Ren, “A double-blockchain solution for agricultural sampled data based on Ethereum and MPT enhancements”, *Future Generation Computer Systems*, iss. 117, pp. 48-58, 2021. doi: https://doi.org/10.1016/j.future.2020.08.036.
[7] L. Zhang, Q. Zhao, and M. Liu, “Towards efficient integration of blockchain for IoT security: The case study of IoT remote access”, *Future Generation Computer Systems*, iss. 116, pp. 215-228, 2021. doi: https://doi.org/10.1016/j.future.2020.10.024.
[8] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, “On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance”, *Computer Networks*, iss. 191, art. 108005, 2021. doi: https://doi.org/10.1016/j.comnet.2021.108005.
[9] B. Cao, Y. Li, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, “When Internet of Things meets blockchain: Challenges in distributed consensus”, *IEEE Network*, vol. 33, no. 6, pp. 133-139, 2019. doi: https://doi.org/10.1109/MNET.2019.1900002.
[10] “What are Patricia Merkle Tries?”, *Alchemy Labs*, 2025. [Електронний ресурс]. Доступно: https://alchemy.com/docs/patricia-merkle-tries. Дата звернення: Серп. 14, 2025.
[11] “Merkle Patricia Tries: A deep dive into data structure security”, *Cardano Foundation*, 2025. [Електронний ресурс]. Доступно: https://cardanofoundation.org/blog/merkle-patricia-tries-deep-dive. Дата звернення: Серп. 10, 2025.
[12] “Merkle-Patricia Trie data structure overview”, *Ethereum Foundation*, 2025. [Електронний ресурс]. Доступно: https://ethereum.org/en/developers/docs/data-structures-and-encoding/patricia-merkle-trie. Дата звернення: Серп. 10, 2025.
[13] K. Ježek, “Ethereum data structures: Merkle Patricia Trie and performance challenges”, *Journal of Blockchain Research*, vol. 2, no. 1, pp. 45-56, 2021. doi: https://doi.org/10.48550/arXiv.2108.05513.

Стаття надійшла до редакції 12.10.2025 р.

REFERENCES

[1] I. Zarudny, and V. Lyubchak, “Methods and information technologies for secure integration of the Ethereum blockchain with the Internet of Things (IoT)”, *Cybersecurity: Education, Science, Technology*, vol. 4, no. 28, pp. 104-114, 2025. doi: https://doi.org/10.28925/2663-4023.2025.28.758.
[2] V. Balatska, and I. Opirsky, “Ensuring the confidentiality of personal data and supporting cybersecurity using blockchain”, *Cybersecurity: Education, Science, Technology*, vol. 4, no. 20, pp. 6-19, 2023. doi: https://doi.org/10.28925/2663-4023.2023.20.619.
[3] V. Mardiansyah, A. Muis, and R.F. Sari, “Multi-State Merkle Patricia Trie (MSMPT): High-performance data structures for multi-query processing based on lightweight blockchain”, *IEEE Access*, iss. 11, pp. 1-14, 2023. doi: https://doi.org/10.1109/ACCESS.2023.3325748.
[4] Y. Deng, M. Yan, and B. Tang, “Accelerating Merkle Patricia Trie with GPU”, in *Proc. VLDB Endowment*, vol. 17, no. 8, pp. 1856-1869, 2024. doi: https://doi.org/10.14778/3659437.3659443.
[5] J. Xu, Y. Tian, T. Ma, and N. Al-Nabhan, “Intelligent manufacturing security model based on improved blockchain”, *Mathematical Biosciences and Engineering*, vol. 17, no. 5, c. 5633-5650, 2020. doi: https://doi.org/10.3934/mbe.2020303.
[6] W. Ren, “A double-blockchain solution for agricultural sampled data based on Ethereum and MPT enhancements”, *Future Generation Computer Systems*, iss. 117, pp. 48-58, 2021. doi: https://doi.org/10.1016/j.future.2020.08.036.
[7] L. Zhang, Q. Zhao, and M. Liu, “Towards efficient integration of blockchain for IoT security: The case study of IoT remote access”, *Future Generation Computer Systems*, iss. 116, pp. 215-228, 2021. doi: https://doi.org/10.1016/j.future.2020.10.024.

[8] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, “On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance”, *Computer Networks*, iss. 191, art. 108005, 2021. doi: https://doi.org/10.1016/j.comnet.2021.108005.
[9] B. Cao, Y. Li, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, “When Internet of Things meets blockchain: Challenges in distributed consensus”, *IEEE Network*, vol. 33, no. 6, pp. 133-139, 2019. doi: https://doi.org/10.1109/MNET.2019.1900002.
[10] “What are Patricia Merkle Tries?”, *Alchemy Labs*, 2025. [Online]. Available: https://alchemy.com/docs/patricia-merkle-tries. Accessed on: Aug. 14, 2025.
[11] “Merkle Patricia Tries: A deep dive into data structure security”, *Cardano Foundation*, 2025. [Online]. Available: https://cardanofoundation.org/blog/merkle-patricia-tries-deep-dive. Accessed on: Aug. 10, 2025.
[12] “Merkle-Patricia Trie data structure overview”, *Ethereum Foundation*, 2025 [Online]. Available: https://ethereum.org/en/developers/docs/data-structures-and-encoding/patricia-merkle-trie. Accessed on: Aug. 10, 2025.
[13] K. Ježek, “Ethereum data structures: Merkle Patricia Trie and performance challenges”, *Journal of Blockchain Research*, vol. 2, no. 1, pp. 45-56, 2021. doi: https://doi.org/10.48550/arXiv.2108.05513.

IVAN ZARUDNY,
VOLODYMYR LYUBCHAK

SELECTION OF ALGORITHMS AND DATA STRUCTURES FOR SECURE STORAGE AND PROCESSING OF METADATA IN IOT SYSTEMS BASED ON THE ETHEREUM BLOCKCHAIN

Abstract. The article examines the theoretical foundations for selecting algorithms and data structures to ensure secure storage and processing of metadata in IoT systems using the Ethereum blockchain. A classification of metadata types specific to heterogeneous IoT environments is presented, taking into account semantic significance, update frequency, and data criticality. Formal requirements for algorithms are formulated, covering resistance to forgery, computational complexity, scalability under high-intensity request loads, and resource efficiency in terms of gas costs and network throughput. A comparative analysis of data structures employed in the Ethereum infrastructure, including Merkle Tree, Merkle-Patricia Trie (*MPT*), Multi-State *MPT*, and *GPU*-accelerated modifications, is performed according to criteria such as asymptotic complexity, memory efficiency, and suitability for incremental updates. A conceptual model for organizing metadata exchange between IoT nodes and smart contracts is proposed, incorporating modules for encoding, verification, gas cost optimization, and standardized interaction interfaces. The presented results provide a theoretical basis for developing formally verified and energy-efficient solutions in the field of secure Ethereum blockchain integration with the Internet of Things.

Keywords: Internet of Things; Ethereum blockchain; metadata processing algorithms; Merkle-Patricia Trie; data structures; cryptographic verification; gas efficiency.

Зарудний Іван Сергійович, аспірант, Сумський Державний Університет, Суми, Україна. ORCID 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 0000-0002-7335-6716. v.liubchak@dcs.sumdu.edu.ua.

Zarudny Ivan, postgraduate student, Sumy State University, Sumy, Ukraine.

Lyubchak Volodymyr, candidate of physical and mathematical sciences, associate professor, head of the department of cybersecurity, Sumy State University, Sumy, Ukraine.