



DOI 10.28925/2663-4023.2026.35.1374

УДК 004.75:004.4

Гавор Артур Станіславович

старший викладач кафедри технологій цифрового розвідку.

Державний університет інформаційно-комунікаційних технологій, Київ, Україна

ORCID: 0009-0002-9705-1666

a.havor@duikt.edu.ua

Шлянчак Світлана Олександрівна

доцент кафедри інформаційних та цифрових технологій

Центральноукраїнський державний університет імені Володимира Винниченка, Кропивницький, Україна

ORCID: 0000-0001-9893-5709

shlanchaksveta@gmail.com

Аносов Андрій Олександрович

доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимир Бурячка

Київський столичний університет імені Бориса Грінченка, Київ, Україна

ORCID: 0000-0002-2973-6033

a.anosov@kubg.edu.ua

**ОСОБЛИВОСТІ ОПТИМІЗАЦІЇ ТРАНЗАКЦІЙНИХ ВИТРАТ СМАРТ-КОНТРАКТІВ У
ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ МОНІТОРИНГУ НА БАЗІ EVM**

Анотація. У статті досліджено проблему економічної неефективності прямої інтеграції мереж Інтернету речей (IoT) із децентралізованими блокчейн-платформами через високі комісійні витрати, що тарифікуються в одиницях газу (Gas) віртуальної машини Ethereum (EVM). Актуальність роботи зумовлена зростанням обсягів багатовимірної телеметрії у системах моніторингу критичної інфраструктури та необхідністю забезпечення незмінності аудиторського сліду без швидкого вичерпання лімітів блоку мережі. Показано, що традиційні моделі On-chain верифікації та стандартного ABI-кодування мають лінійну асимптотичну складність транзакційних витрат і призводять до марнотратного використання енергонезалежного сховища (SSTORE) через ефект роздування вхідних даних (Calldata Bloat). Запропоновано комплексний підхід до мінімізації вартості транзакцій у середовищі EVM, що базується на винесенні процедур перевірки консенсусного кворуму в позамережеве середовище (Off-chain) за допомогою порогової криптографії та застосуванні алгоритму побітового ущільнення змінних стану (Bitwise Slot Packing). Розроблено архітектуру взаємодії смарт-контракту з периферійним шлюзом, де верифікація зведеного вектора здійснюється за допомогою єдиного виклику прекомпільованого примітиву esgcover. Особливістю підходу є консолідація незалежних 16-бітних сенсорних метрик в одне 256-бітне машинне слово за допомогою логічних операторів побітового зсуву, що дозволяє підвищити корисну інформаційну щільність слота пам'яті. Практична цінність розробленої моделі полягає у переведенні обчислювальної складності верифікації смарт-контракту в константний клас $O(1)$ та підтвердженню зниженні транзакційних витрат на 98%. Це дозволяє використовувати публічні та консорціумні блокчейн-мережі як рентабельний рівень аудиту для систем екологічного та індустріального моніторингу.

Ключові слова: смарт-контракт; віртуальна машина Ethereum; EVM; оптимізація газу; Інтернет речей; побітове пакування; пороговий підпис.

ВСТУП

Інтенсивна цифровізація об'єктів критичної інфраструктури, промислових підприємств та комплексів екологічного контролю супроводжується масовим розгортанням бездротових сенсорних мереж Інтернету речей (IoT) [1], [2]. Для гарантування цілісності, прозорості та неможливості ретроспективної підробки зібраних телеметричних показників дедалі ширше застосовуються технології розподіленого реєстру (блокчейн) та смарт-контракти, сумісні з середовищем виконання Ethereum Virtual



Machine (EVM) [3], [4]. У такій конфігурації блокчейн виступає децентралізованим рівнем довіри, який фіксує незмінний аудиторський слід стану контрольованого середовища [5].

Разом із тим практична експлуатація EVM-сумісних реєстрів у задачах високочастотного моніторингу стикається з жорстким економічним та пропускним бар'єром – високою вартістю виконання обчислювальних інструкцій та збереження стану, що тарифікується в одиницях газу (Gas) [6], [7]. Оскільки розподілені сенсорні мережі генерують неперервні потоки багатовимірних даних, застосування класичних підходів із прямою фіксацією відліків від кожного пристрою призводить до стрімкого переповнення лімітів блоку та економічної нерентабельності системи [8].

Постановка проблеми. У традиційних децентралізованих системах моніторингу взаємодія периферійного рівня з блокчейн-реєстром реалізується або шляхом індивідуального надсилання транзакцій кожним сенсорним вузлом, або через верифікацію масиву мультипідписів безпосередньо всередині смарт-контракту (On-chain) [4], [9]. Обидві парадигми характеризуються лінійною асимптотичною складністю транзакційних витрат $O(N)$ відносно кількості пристроїв у кластері $\square$. Відповідно до специфікації віртуальної машини EVM, кожна операція ініціалізації нового 256-бітного слота в енергонезалежному сховищі стану (SSTORE) вимагає базових 20000 Gas, а побайтова передача вхідних параметрів виклику (Calldata) створює додаткове фінансове навантаження [6].

Водночас проблема суттєво поглиблюється структурною надлишковістю стандартного бінарного кодування інтерфейсів (ABI Encoding) у мові Solidity [7], [8]. Оцифровані показники фізико-хімічних або промислових датчиків після цілочисельного масштабування зазвичай мають розрядність 16 бітів (2 байти). Проте архітектура EVM оперує неподільними 256-бітними машинними словами (32 байти), внаслідок чого кожен переданий параметр масиву автоматично доповнюється 240 незначущими нульовими бітами (Zero Padding) [8]. Це призводить до явища роздування транзакційних даних (Calldata Bloat), за якого корисне інформаційне навантаження слота становить лише 6,25%, тоді як комісія мережі стягується за весь зарезервований обсяг пам'яті. Отже, виникає науково-прикладне протиріччя між необхідністю криптографічно достовірної фіксації багатовимірної телеметрії від масштабних IoT-кластерів та жорсткими обмеженнями обчислювальних ресурсів віртуальної машини блокчейну.

Аналіз останніх досліджень і публікацій. Питанням архітектурної інтеграції мереж Інтернету речей із блокчейн-платформами та оптимізації витрат смарт-контрактів присвячено значну кількість сучасних наукових праць [1]–[12]. Зокрема, у фундаментальних оглядах хмарних та периферійних обчислень для промислового Інтернету речей [1], [2] обґрунтовано доцільність попередньої обробки телеметрії на крайовому рівні (Edge Layer) для розвантаження магістральних каналів зв'язку. У дослідженні [3] запропоновано модель децентралізованого управління ідентичністю IoT-пристроїв у критичних інфраструктурах на базі хмарних сервісів і блокчейн-реєстрів, яка дозволяє делегувати ресурсомісткі операції верифікації на периферійні вузли. Проте в зазначених роботах основну увагу зосереджено на автентифікації вузлів та мережевих затримках, тоді як проблема мінімізації вартості збереження багатовимірних телеметричних векторів у пам'яті віртуальної машини залишається поза увагою.

У працях, присвячених архітектурі блокчейн-оракулів та гібридним протоколам взаємодії [4], [5], проаналізовано механізми доставки зовнішніх сенсорних даних до смарт-контрактів. Авторами роботи [4] показано, що централізовані оракули створюють критичну вразливість єдиної точки відмови (Single Point of Failure), тоді як у дослідженні [5] запропоновано адаптивні низьколатентні технології обміну даними між позамережевим (Off-chain) та мережевим (On-chain) рівнями. Подальший розвиток цього напрямку відображено у роботі [12], де сформульовано архітектурну модель відмовостійкої інтеграції периферійних IoT-мереж із блокчейн-реєстрами, що створює теоретичне підґрунтя для децентралізованої консолідації потоків телеметрії.

Питання безпосереднього профілювання та зниження витрат газу в середовищі EVM детально розглянуто у дослідженнях [6]–[8]. У роботах [6], [7] проведено систематичний аналіз інструментів статичного аудиту смарт-контрактів та емпіричне оцінювання патернів газової оптимізації на рівні байт-коду Solidity (зокрема використання незмінних констант immutable, заміна динамічних масивів фіксованими структурами та пряме читання буфера calldata). Однак такі прийоми забезпечують лише локальне скорочення витрат у межах 10–15% і не вирішують проблеми лінійного масштабування вартості транзакцій $\square(\square)$ при зростанні кількості датчиків. Найбільш близьким за постановкою є дослідження [8], у якому запропоновано зменшувати газову вартість зберігання IoT-телеметрії в Ethereum шляхом побітового пакування та пакування у мережах другого рівня (Rollups). Разом із тим у праці [8] не розглянуто механізми криптографічного підтвердження групового консенсусу периферійних вузлів перед пакуванням даних.

Для вирішення задачі групової криптографічної верифікації у роботах [9]–[11] досліджуються порогові схеми електронного підпису (Threshold Signature Schemes – TSS) на еліптичних кривих. У праці



[9] та дорожній карті інституту стандартів NIST [10] формалізовано критерії стійкості порогових примітивів ECDSA, які дозволяють групі вузлів генерувати єдиний сумісний підпис фіксованої довжини без відновлення закритого ключа в одній точці. У роботі [11] досліджено асинхронні репутаційно-зважені протоколи візантійського консенсусу для масштабних IoT-мереж, що забезпечують достовірне узгодження даних на периферії.

Незважаючи на вагомий науковий доробок, питання синергетичного поєднання позамережевої порогової агрегації підписів за допомогою прекомпільованого примітиву `esgcover` із низькорівневим побітовим ущільненням багатовимірних векторів телеметрії у 256-бітні слоти EVM та каскадною On-chain валідацією залишається недостатньо розробленим, що визначає актуальність даної статті.

Мета статті. Метою дослідження є підвищення економічної рентабельності та масштабованості децентралізованих інформаційних систем моніторингу шляхом розробки методів та алгоритмів мінімізації транзакційних витрат смарт-контрактів у середовищі EVM. Для досягнення поставленої мети необхідно вирішити такі задачі:

- проаналізувати структуру формування витрат газу в архітектурі EVM при обробці багатовимірних потоків телеметрії та визначити чинники інформаційної надлишковості;
- розробити архітектурну модель позамережевої консолідації транзакцій на основі порогових криптографічних схем та прекомпільованих примітивів;
- формалізувати метод та алгоритм побітового ущільнення змінних стану у 256-бітному машинному слові з контролем розрядності;
- розробити алгоритм каскадної верифікації транзакцій та сценарної обробки телеметрії у смарт-контракті;
- провести експериментальне профілювання розробленого смарт-контракту та оцінити досягнутий рівень економії обчислювальних ресурсів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Дослідження базується на концепціях децентралізованих систем, технологій розподіленого реєстру, крайових обчислень (Edge Computing) та криптографічного захисту даних у середовищі віртуальної машини Ethereum (EVM).

В основі роботи лежать такі ключові терміни, поняття та категорії:

1. Віртуальна машина Ethereum (Ethereum Virtual Machine, EVM) – децентралізоване середовище виконання смарт-контрактів, у якому кожна обчислювальна операція та модифікація стану тарифікуються в одиницях газу (Gas).
2. Порогова схема підпису (Threshold Signature Scheme, TSS) – криптографічний підхід, за якого приватний ключ розподіляється між вузлами кластера, що дозволяє формувати єдиний верифікований підпис без розкриття повного ключа.
3. Побітове пакування (Bitwise Slot Packing) – метод структурної оптимізації пам'яті смарт-контрактів, що полягає в консолідації кількох змінних меншої розрядності в єдине 256-бітне машинне слово `uint256` для уникнення надлишкового нульового доповнення (Zero Padding).
4. Прекомпільовані примітиви (Precompiled Contracts) – вбудовані криптографічні функції EVM (зокрема `esgcover`), що виконуються поза загальною віртуальною машиною з жорстко зафіксованою та зниженою вартістю у газі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для зниження транзакційних витрат у блокчейн-мережах на базі EVM було розроблено двоетапний механізм оптимізації, який охоплює архітектурне винесення перевірки кворуму в позамережеве середовище (Off-chain) та низькорівнєве управління пам'яттю смарт-контракту.

Класичний підхід до децентралізованого моніторингу вимагає від смарт-контракту циклічної перевірки масиву криптографічних підписів від кожного IoT-датчика або запису даних у цикл `SSTORE`. Це зумовлює лінійну асимптотичну складність транзакційних витрат $O(N)$.

Для подолання цього обмеження запропоновано архітектуру, де ресурсомісткі задачі делегуються периферійному шлюзу (Edge Gateway). Вузли кластера локально формують єдиний пороговий підпис (Threshold Signature Scheme) $Sig = (v, r, s)$ для агрегованого вектора телеметрії. Смарт-контракт отримує вже консолідований пакет і замість циклічної верифікації викликає прекомпільований примітив `esgcover` лише один раз.

На схемі відображено структурну різницю між двома підходами до взаємодії з розподіленим реєстром. У традиційній моделі смарт-контракт змушений виконувати ітеративний цикл перевірки

підписів та численні операції запису в пам'ять, тоді як запропонована модель переносить агрегацію на периферійний шлюз і зводить роботу віртуальної машини до однієї перевірки умови та одного запису в реєстр.

Вартість виконання *esrecovers* у віртуальній машині Ethereum жорстко зафіксована жовтою книгою (Ethereum Yellow Paper) на рівні 3000 Gas. Разом із базовою вартістю ініціалізації транзакції та одним записом у сховище стану, теоретична функція витрат системи стає константною:

$$\begin{cases} G_{classic}(N) = G_{base} + N \cdot (G_{verify} + G_{SSTORE}) = O(N), \\ G_{opt} = G_{base} + G_{ecrecover} + G_{SSTORE} + G_{calldata} = O(1), \end{cases} \quad (1)$$

де $G_{classic}(N)$ – сумарні витрати газу в традиційній архітектурі при опитуванні $\square$ сенсорних вузлів; G_{opt} – сумарна оптимізована вартість транзакції в одиницях газу за запропонованим методом; G_{base} – базова вартість ініціалізації транзакції в мережі EVM; G_{verify} – витрати екомпільованого контракту відновлення публічного ключа з порогового підпису (на індивідуальну перевірку підпису одного вузла; $G_{ecrecover}$ – фіксована вартість виклику прекомпільованого контракту відновлення публічного ключа з порогового підпису; G_{SSTORE} – вартість ініціалізації 256-бітного слота в енергонезалежному сховищі стану; $G_{calldata}$ – витрати на передачу стисненого вхідного пакета даних.

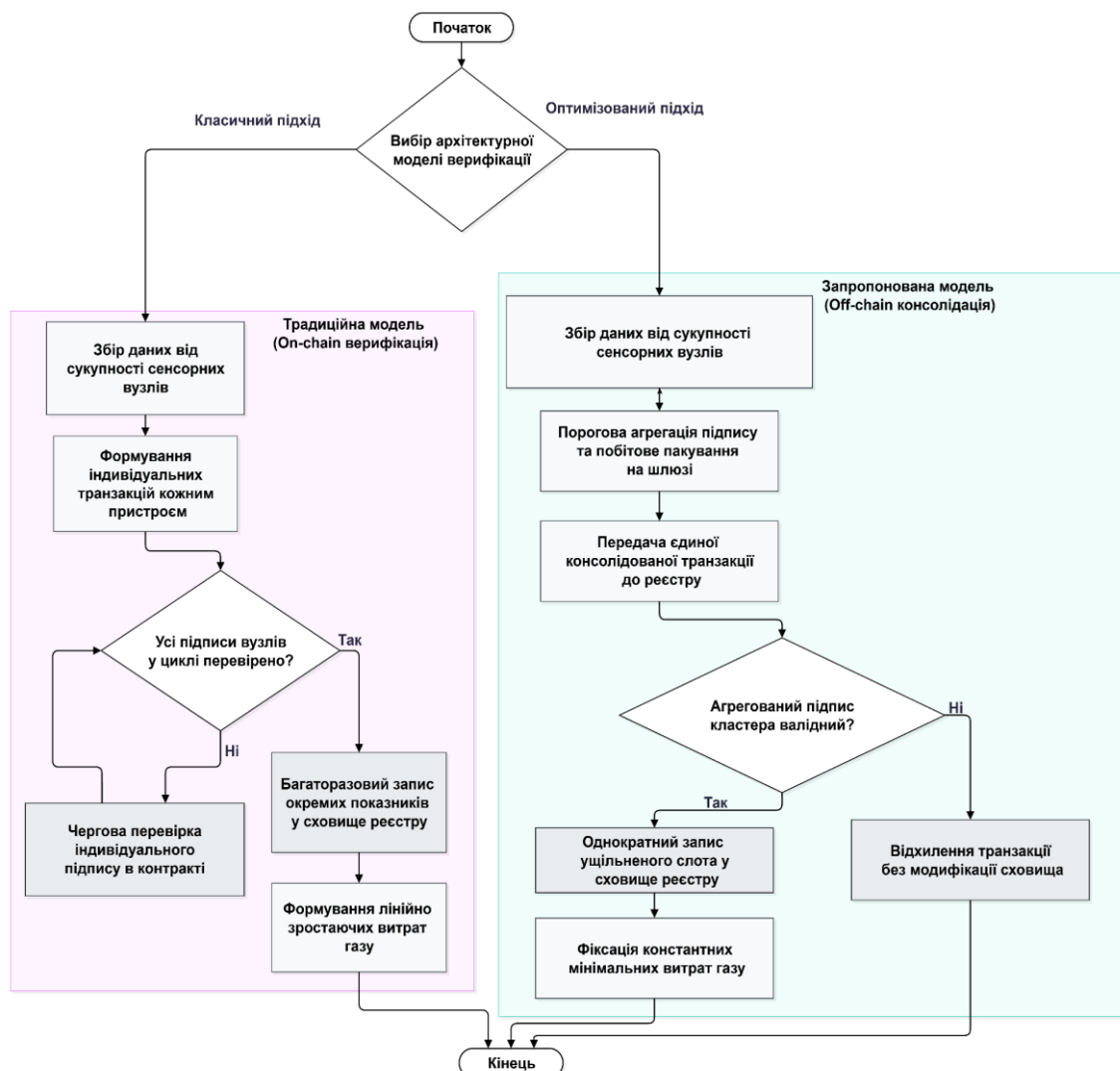


Рис. 1. Порівняльна блок-схема організації процесів верифікації телеметрії у традиційній та запропонованій архітектурах



Другим рівнем оптимізації є ліквідація проблеми роздування вхідних даних (Calldata Bloat) та марнотратства енергонезалежної пам'яті за допомогою методу побітового ущільнення змінних стану (Bitwise Slot Packing). Оскільки для високоточного представлення квантованих параметрів моніторингу достатньо 16-бітної розрядності (діапазон значень від 0 до 65535), один 256-бітний регістр віртуальної машини здатний вмістити до 16 незалежних параметрів.

Алгоритмічно ущільнення виконується на стороні крайового шлюзу за допомогою операторів побітового зсуву вліво (<<) та логічного «АБО» (|). У смарт-контракті замість збереження масиву ініціалізується єдина змінна uint256 payload. Якщо логіка контракту вимагає зчитування окремого параметра для генерації події (Event), застосовується бітова маска (0xFFFF) та зсув вправо (>>).

На стороні периферійного шлюзу кожен вимірюваний фізичний параметр масштабується до беззнакового 16-бітного цілого числа і розміщується у відповідній позиції 256-бітного слова за допомогою побітового зсуву вліво. Математично операція пакування вектора з k параметрів ($k \leq 16$) визначається виразом:

$$Payload = \bigcup_{i=1}^k ((p_i \& 0xFFFF) \ll 16 \cdot (i - 1)), \quad (2)$$

де *Payload* – фінальне 256-бітне машинне слово (змінна типу uint256), що містить ущільнений вектор телеметрії; k – загальна кількість параметрів моніторингу у векторі; p_i – i -й масштабований цілочисельний параметр телеметрії; i – порядковий індекс параметра у векторі ($i = \overline{1, k}$).

Якщо внутрішня бізнес-логіка смарт-контракту вимагає перевірки окремого показника безпосередньо під час виконання транзакції (наприклад, для контролю перевищення аварійних нормативів), зворотне декодування i -го параметра здійснюється за константний час у регістровій пам'яті за формулою:

$$p_i = (Payload \gg 16 \times (i - 1)) \& 0xFFFF, \quad (3)$$

де >> – оператор побітового зсуву вправо на $16 \cdot (i - 1)$ позицій, який переміщує цільове 16-бітне поле у молодші розряди машинного слова перед накладанням маски 0xFFFF.

Структурну схему розподілу бітового простору 256-бітного слота пам'яті при стандартному кодуванні та запропонованому побітовому ущільненні подано на рис. 2.

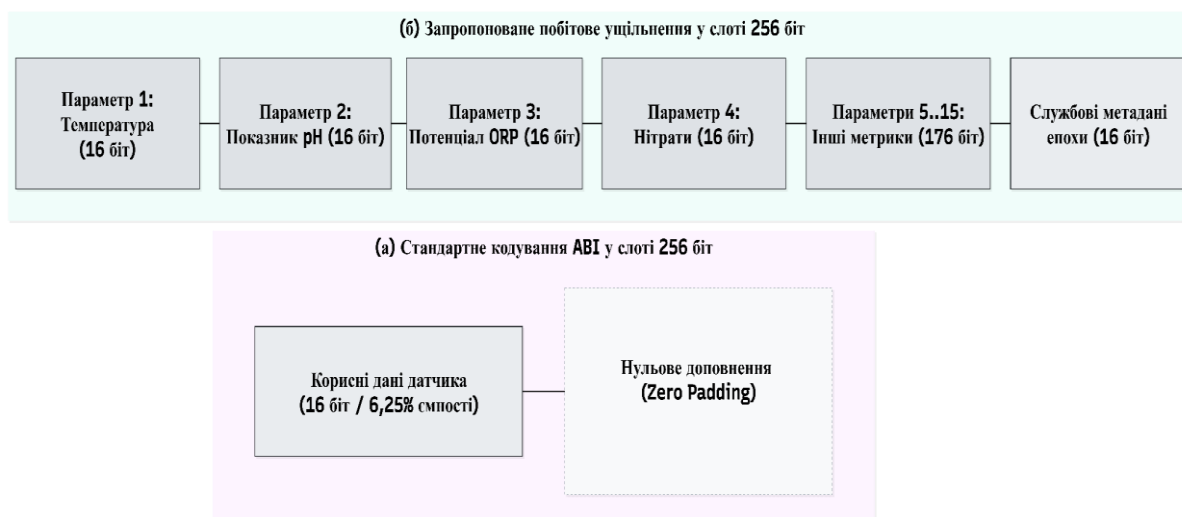


Рис. 2. Структурна схема використання розрядів 256-бітного машинного слова EVM: (а) стандартне кодування без ущільнення; (б) запропоноване побітове пакування

На схемі відображено механізм ліквідації структурної надлишковості пам'яті. Замість збереження одного 16-бітного показника з 240 порожніми нульовими бітами, побітове ущільнення консолідує до п'ятнадцяти вимірюваних параметрів та блок службових метаданих епохи в єдиний слот, підвищуючи корисну інформаційну щільність до 93,75–100%.

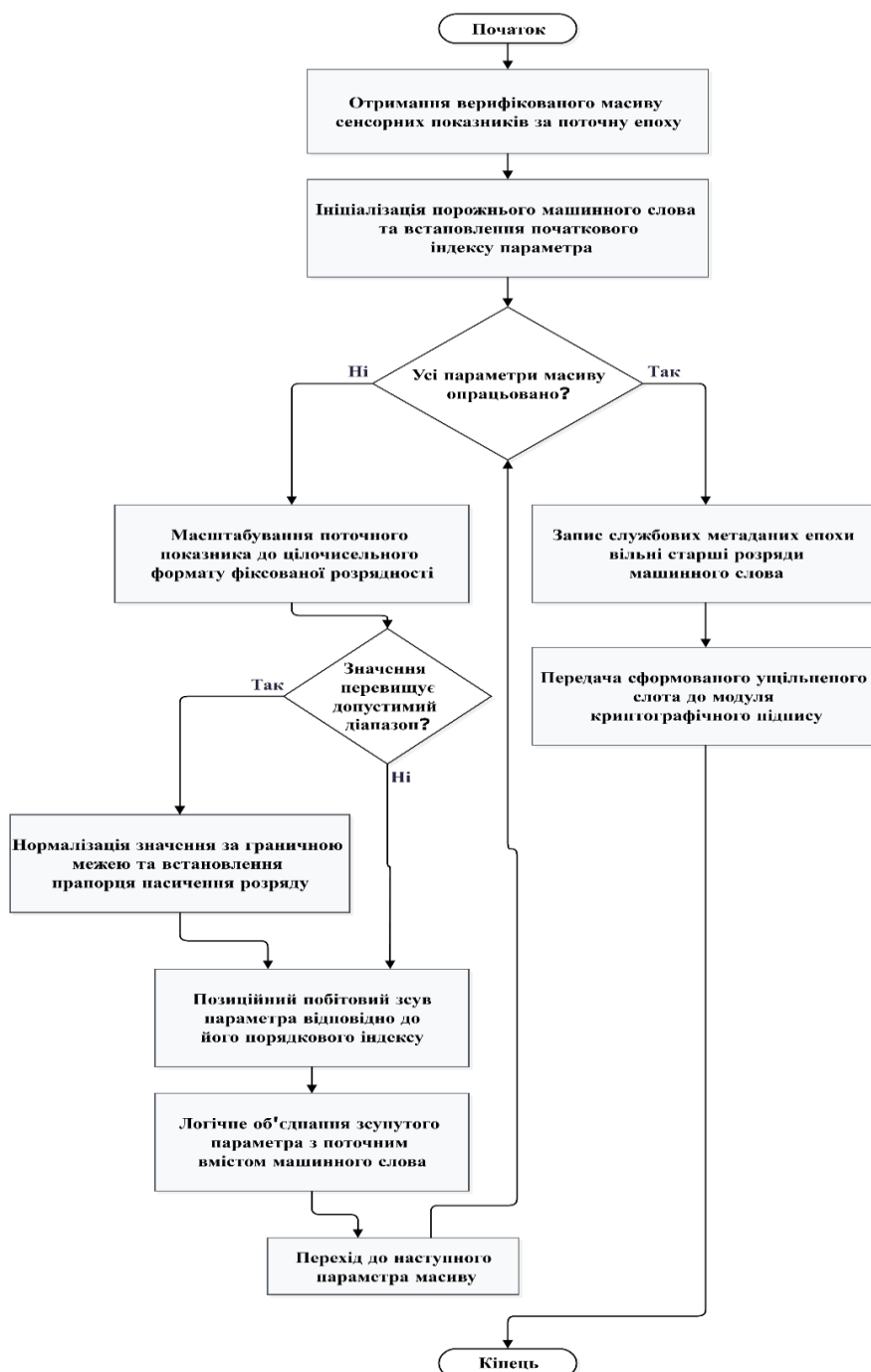


Рис. 3. Блок-схема алгоритму побітового ущільнення телеметрії у слот пам'яті

Для програмної реалізації описаного математичного апарату на рівні периферійного шлюзу розроблено ітеративний алгоритм побітового ущільнення з контролем виходу значень за межі розрядності, блок-схема якого наведена на рис. 3.

На схемі відображено циклічну процедуру формування консолідованого слота на периферійному вузлі. Обов'язкова перевірка діапазону значень перед побітовим зсувом унеможливорює арифметичне переповнення розрядів, при якому старші біти одного параметра могли б пошкодити сусіднє поле у 256-бітному регістрі.

Функціонування всієї запропонованої системи оптимізації транзакційних витрат визначається послідовністю взаємопов'язаних операцій, які охоплюють повний цикл обробки телеметрії – від моменту збору первинних показників у розподіленому середовищі до їх незмінної фіксації у блокчейн-реєстрі.

Алгоритм базується на узгодженій взаємодії між сенсорними пристроями, периферійним шлюзом, смарт-контрактом віртуальної машини та аналітичними сервісами і передбачає поетапну агрегацію, ущільнення та каскадну перевірку достовірності даних.

Початковим етапом є ініціалізація чергової епохи моніторингу та збір первинних показників від вузлів кластера. Отримані відліки передаються на периферійний рівень для локальної фільтрації та перевірки досягнення необхідного порогового кворуму. Якщо кворум пристроїв не досягнуто протягом визначеного інтервалу очікування, епоха відхиляється на рівні шлюзу без звернення до блокчейн-мережі, що запобігає непродуктивним витратам обчислювальних ресурсів реєстру. За умови наявності кворуму периферійний вузол виконує побітове ущільнення багатовимірної масиви показників у єдиний слот пам'яті та формує спільний пороговий підпис, після чого консолідована транзакція надсилається до блокчейн-мережі.

У процесі верифікації на рівні смарт-контракту виконується багатоступенева перевірка вхідної транзакції за принципом раннього відхилення некоректних запитів (Fail-Fast). Спочатку перевіряється актуальність часової мітки та порядкового номера пакета (nonce) для захисту від атак повторного відтворення раніше перехоплених транзакцій (Replay Attacks). На наступному кроці здійснюється перевірка канонічності криптографічного підпису та відновлення адреси підписанта за допомогою прекомпільованого примітиву віртуальної машини. У разі виявлення невідповідності на будь-якому з етапів перевірки транзакція негайно скасовується інструкцією Revert без виконання ресурсомісткої операції запису в енергонезалежне сховище.

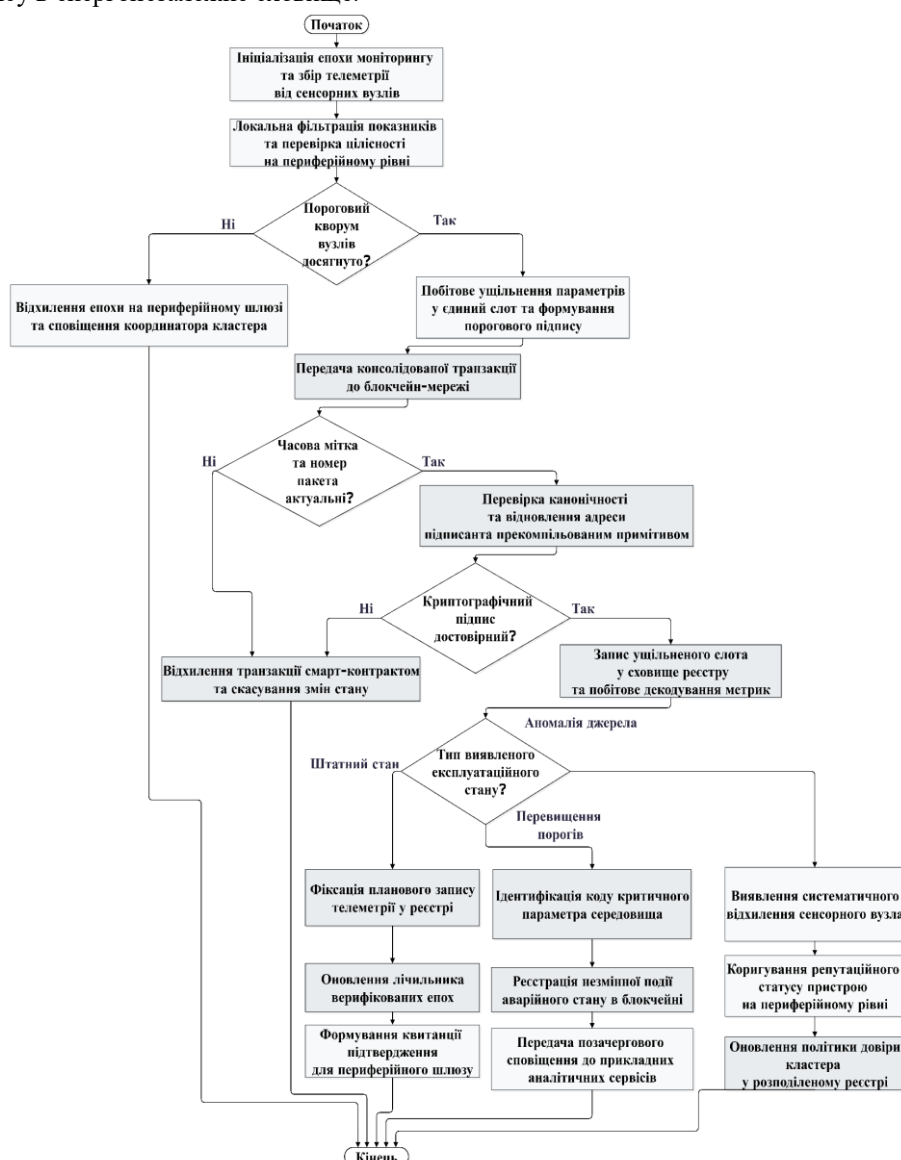


Рис. 4. Алгоритм функціонування системи та каскадної верифікації транзакцій



Після успішного підтвердження автентичності ущільнений слот записується до реєстру, а смарт-контракт виконує побітове декодування контрольних показників. Виділено три ключові сценарії подальшого функціонування системи залежно від результатів аналізу декодованого стану. У режимі штатного моніторингу, коли всі показники перебувають у межах норми, здійснюється стандартна фіксація запису, оновлення лічильника епох та повернення квитанції підтвердження на периферійний шлюз. У разі виявлення перевищення гранично допустимих порогів ідентифікується код критичного параметра, у блоке реєструється незмінна подія тривоги та формується позачергове сповіщення для прикладних аналітичних служб. Якщо ж під час узгодження виявляється систематичне відхилення у поведінці окремого джерела даних, ініціюється сценарій коригування його репутаційного статусу з відповідним оновленням політики довіри кластера. Загальна логіка роботи системи представлена на рис. 4.

На схемі відображено послідовність дій від моменту збору сенсорних даних до їх перевірки у смарт-контракті та розгалуження за трьома експлуатаційними сценаріями, що дозволяє описати поведінку системи в умовах динамічного середовища та мінімізувати накладні витрати реєстру.

Для кількісного оцінювання ефективності запропонованих рішень розгорнуто локальне імітаційне середовище віртуальної машини Ethereum на базі фреймворку Hardhat. Експериментальне профілювання транзакційних витрат (Gas Cost) проводилося для сценарію фіксації 7-вимірного вектора телеметрії при масштабуванні розміру сенсорного кластера N у діапазоні від 10 до 100 вузлів. Результати порівняльного аналізу класичного On-chain підходу, проміжного варіанта без побітового пакування та запропонованого комплексного методу наведено у табл. 1.

Таблиця 1

Порівняльний аналіз транзакційних витрат (Gas) залежно від розміру IoT-кластера

Кількість датчиків у кластері (N), од	Класичний підхід On-chain $O(N)$, Gas	Пороговий підпис без пакування, Gas	Запропонований метод, Gas	Відносна економія газу, %
10	221 000	182 200	46 100	79,14%
30	621 000	182 200	46 100	92,58%
50	1 021 000	182 200	46 100	95,48%
70	1 421 000	182 200	46 100	96,76%
100	2 021 000	182 200	46 100	97,72%

Графічну інтерпретацію експериментальної асимптотики транзакційних витрат залежно від кількості сенсорних пристроїв у кластері подано на рис. 5.

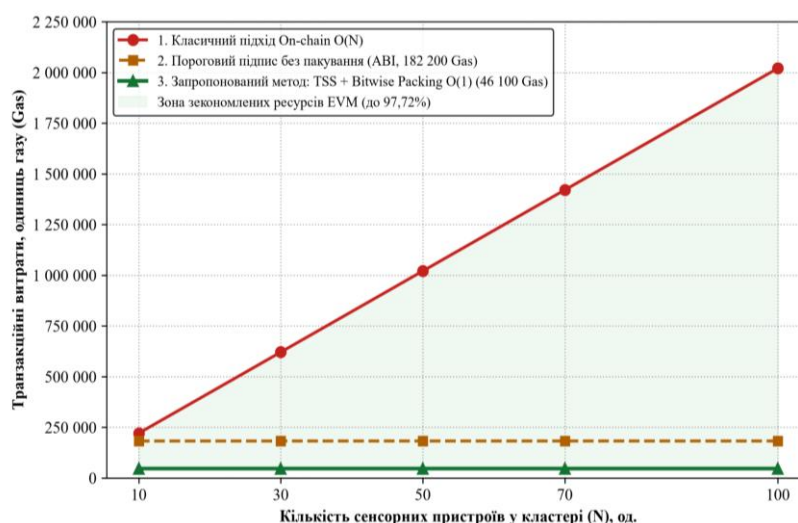


Рис. 5. Динаміка транзакційних витрат газу при масштабуванні сенсорного кластера для різних архітектурних конфігурацій



На графіку відображено три характерні траєкторії витрат обчислювальних ресурсів віртуальної машини: верхня лінійно висхідна крива відповідає класичній On-chain верифікації індивідуальних транзакцій, середня горизонтальна лінія на рівні 182,200 ілюструє застосування порогового підпису при стандартному ABI-кодуванні семи слотів, а нижня горизонтальна пряма на рівні 46,100 демонструє роботу запропонованого методу з побітовим ущільненням.

Порівняльний аналіз отриманих емпіричних даних показує, що класична архітектура при масштабуванні до 100 вузлів вимагає 2,021,000 на кожну епоху моніторингу, що призводить до швидкого вичерпання пропускної здатності блоку. Застосування лише криптографічної агрегації без побітового пакування стабілізує витрати на позначці 182,200, з яких 140,000 витрачається на ініціалізацію семи окремих слотів сховища. Натомість запропонована синергетична модель скорочує витрати у 3,95 раза порівняно зі стандартним ABI-кодуванням та забезпечує 97,72% загальної економії газу при $N = 100$, повністю усуваючи залежність вартості смарт-контракту від фізичної кількості датчиків у мережі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено комплексний підхід до оптимізації транзакційних витрат смарт-контрактів у децентралізованих системах моніторингу, що функціонують на базі віртуальної машини Ethereum (EVM). Запропоноване рішення орієнтоване на подолання ключових обмежень прямої інтеграції мереж Інтернету речей із блокчейн-реєстрами, зокрема лінійного зростання вартості верифікації при масштабуванні кластера та марнотратства енергонезалежної пам'яті внаслідок нульового доповнення стандартних типів даних.

У дослідженні представлено архітектурну модель позамережевої консолідації транзакцій, у якій перевірка кворуму делегується периферійному рівню за допомогою порогових схем підпису, а смарт-контракт виконує однократний виклик прекомпільованого примітиву `ecrecover`. Формалізовано математичну модель та ітеративний алгоритм побітового ущільнення багатовимірних векторів телеметрії у єдине 256-бітне машинне слово, що підвищило корисну інформаційну щільність слота з 6,25% до 93,75%. Розроблено алгоритм каскадної верифікації та сценарної обробки транзакцій, який забезпечує раннє відсікання невалідних запитів та підтримує режими штатного моніторингу, аварійного сповіщення і коригування довіри до вузлів.

Практична цінність запропонованої моделі полягає у переведенні обчислювальної складності On-chain верифікації у константний клас $O(1)$ на рівні 46,100 та зниженні транзакційних витрат до 97,7% для кластера зі 100 пристроїв. Перспективи подальших досліджень доцільно спрямувати на автоматизоване модульне тестування граничних режимів роботи смарт-контракту та адаптацію розробленого механізму побітового ущільнення до мереж другого рівня (Layer-2 Rollups).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dritsas, E., & Trigka, M. (2025). A survey on the applications of cloud computing in the industrial internet of things. *Big Data and Cognitive Computing*, 9(2), 44. <https://doi.org/10.3390/bdcc9020044>
2. Awosika, A., Shukla, R. M., & Pranggono, B. (2025). A survey for blockchain-enabled resource management in edge, cloud, and next generation wireless networks. *IEEE Access*, 13, 14520–14548. <https://doi.org/10.1109/ACCESS.2025.3531240>
3. Розломий, І. О., Бабенко, В. Г., Науменко, С. В., & Лащевська, Н. О. (2026). Модель децентралізованого управління ідентичністю IoT пристроїв у критичних інфраструктурах на основі хмарних сервісів і блокчейн-реєстрів. *Зв'язок*, (4), 45–56. <https://doi.org/10.31673/2412-9070.2026.046913>
4. Caldarelli, G. (2022). Overview of blockchain oracle research. *Future Internet*, 14(6), 175. <https://doi.org/10.3390/fi14060175>
5. Jin, Y., Huang, D., & Tian, C. (2025). On-chain/off-chain adaptive low-latency network communication technology. *Applied Sciences*, 15(16), 8880. <https://doi.org/10.3390/app15168880>
6. Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. (2022). Ethereum smart contract analysis tools: A systematic review. *IEEE Access*, 10, 57037–57062. <https://doi.org/10.1109/ACCESS.2022.3169902>
7. Pinna, A., Ibba, S., Baralla, G., Tonelli, R., & Marchesi, M. (2021). A massive analysis of Ethereum smart contracts: Empirical gas profiling on local EVM testnets. *IEEE Access*, 9, 78014–78031. <https://doi.org/10.1109/ACCESS.2021.3083836>



8. Vacek, V., Zarb, A., & Ellul, J. (2023). Reducing the gas cost of IoT telemetry storage on Ethereum using bit-packing and Rollup batching. *Blockchain: Research and Applications*, 4(3), 100142. <https://doi.org/10.1016/j.bcr.2023.100142>
9. Aumasson, J. P., Hamelink, A., & Shlomovits, O. (2021). A survey of ECDSA threshold signing. *IACR Cryptology ePrint Archive*, Paper 2020/1390, 1–34. <https://eprint.iacr.org/2020/1390>
10. Brandão, L. T. A. N., Davidson, M., & Vassilev, A. (2023). *NIST roadmap toward criteria for threshold schemes for cryptographic primitives* (NIST Internal Report 8214B). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8214B>
11. Jia, G., Chen, Y., & Li, X. (2025). RWA-BFT: Reputation-weighted asynchronous BFT for large-scale IoT. *Sensors*, 25(2), 413. <https://doi.org/10.3390/s25020413>.
12. Гавор, А. С., & Герцюк, М. М. (2026). Архітектурна модель відмовостійкої інтеграції периферійних IoT-мереж із блокчейн-реєстрами на базі порогової криптографії. *Телекомунікаційні та інформаційні технології*, 92(3), 167–177. <https://doi.org/10.31673/2412-4338.2026.032417>

**Artur Havor**

Senior Lecturer, Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0002-9705-1666
a.havor@duikt.edu.ua

Svitlana Shlianchak

Associate Professor, Department of Information and Digital Technologies
Work place: Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, Ukraine
ORCID: 0000-0001-9893-5709
shlianchaksveta@gmail.com

Andriy Anosov

Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

**FEATURES OF OPTIMIZING TRANSACTION COSTS OF SMART CONTRACTS IN
DECENTRALIZED MONITORING SYSTEMS BASED ON EVM**

Abstract. The article investigates the problem of economic inefficiency in the direct integration of Internet of Things (IoT) networks with decentralized blockchain platforms due to high transaction costs measured in Ethereum Virtual Machine (EVM) Gas. The relevance of the work is driven by the rapid growth of multidimensional telemetry in critical infrastructure monitoring systems and the need to ensure an immutable audit trail without exhausting block gas limits. It is shown that traditional On-chain verification approaches and standard ABI encoding exhibit linear asymptotic cost complexity and lead to wasteful allocation of non-volatile storage (SSTORE) due to the Calldata Bloat effect. A comprehensive optimization approach for the EVM environment is proposed, combining Off-chain threshold signature aggregation (TSS) with a Bitwise Slot Packing algorithm for state variables. The paper presents the interaction architecture between edge gateways and smart contracts, the bit-level structure of consolidated 256-bit words, and an operational cascade verification algorithm covering normal monitoring, critical threshold exceedance alerts, and sensor source anomaly detection. By packing independent 16-bit sensory metrics into a single 256-bit machine word via bitwise shift operations, the useful information density of the memory slot increases from 6.25% to 93.75%. Empirical profiling confirms that the proposed model transitions smart contract verification complexity to the constant class $O(1)$ and reduces transaction costs by up to 97.7%, maintaining a constant 46,100 Gas per epoch regardless of cluster size. The practical value of the approach lies in enabling public and consortium EVM blockchains to serve as a cost-effective, tamper-proof audit layer for environmental and industrial monitoring infrastructures, resolving the fundamental contradiction between data integrity requirements and blockchain resource constraints.

Keywords: smart contract; Ethereum Virtual Machine; EVM; gas optimization; Internet of Things; bitwise packing; threshold signature; edge computing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Dritsas, E., & Trigka, M. (2025). A survey on the applications of cloud computing in the industrial internet of things. *Big Data and Cognitive Computing*, 9(2), 44. <https://doi.org/10.3390/bdcc9020044>
2. Awosika, A., Shukla, R. M., & Pranggono, B. (2025). A survey for blockchain-enabled resource management in edge, cloud, and next generation wireless networks. *IEEE Access*, 13, 14520–14548. <https://doi.org/10.1109/ACCESS.2025.3531240>
3. Rozlomii, I. O., Babenko, V. H., Naumenko, S. V., & Lashchevska, N. O. (2026). Model detsentralizovanoho upravlinnia identychnisti IoT prystroiv u krytychnykh infrastrukturakh na osnovi khmarnykh servisiv i blokcheyn-reiestriv [A model of decentralized identity management of IoT devices in critical infrastructures based on cloud services and blockchain registry]. *Zviyazok*, (4), 45–56. <https://doi.org/10.31673/2412-9070.2026.046913> [in Ukrainian]. [cite: 1, 12]



4. Caldarelli, G. (2022). Overview of blockchain oracle research. *Future Internet*, 14(6), 175. <https://doi.org/10.3390/fi14060175>
5. Jin, Y., Huang, D., & Tian, C. (2025). On-chain/off-chain adaptive low-latency network communication technology. *Applied Sciences*, 15(16), 8880. <https://doi.org/10.3390/app15168880>
6. Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. (2022). Ethereum smart contract analysis tools: A systematic review. *IEEE Access*, 10, 57037–57062. <https://doi.org/10.1109/ACCESS.2022.3169902>
7. Pinna, A., Ibba, S., Baralla, G., Tonelli, R., & Marchesi, M. (2021). A massive analysis of Ethereum smart contracts: Empirical gas profiling on local EVM testnets. *IEEE Access*, 9, 78014–78031. <https://doi.org/10.1109/ACCESS.2021.3083836>
8. Vacek, V., Zarb, A., & Ellul, J. (2023). Reducing the gas cost of IoT telemetry storage on Ethereum using bit-packing and Rollup batching. *Blockchain: Research and Applications*, 4(3), 100142. <https://doi.org/10.1016/j.bcra.2023.100142>
9. Aumasson, J. P., Hamelink, A., & Shlomovits, O. (2021). A survey of ECDSA threshold signing. *IACR Cryptology ePrint Archive*, Paper 2020/1390, 1–34. <https://eprint.iacr.org/2020/1390>
10. Brandão, L. T. A. N., Davidson, M., & Vassilev, A. (2023). *NIST roadmap toward criteria for threshold schemes for cryptographic primitives* (NIST Internal Report 8214B). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8214B>
11. Jia, G., Chen, Y., & Li, X. (2025). RWA-BFT: Reputation-weighted asynchronous BFT for large-scale IoT. *Sensors*, 25(2), 413. <https://doi.org/10.3390/s25020413>
12. Havor, A. S., & Gertsjuk, M. M. (2026). Architectural model of fault-tolerant integration of peripheral iot networks with blockchain ledgers based on threshold cryptography. *Telecommunication and information technologies*, 92(3), 167–177. <https://doi.org/10.31673/2412-4338.2026.032417>

Отримано редакцією журналу / Received: 14.09.26

Прорецензовано / Revised: 24.09.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.