

Гавор Артур Станіславович

старший викладач кафедри Технологій цифрового розвитку

Державний університет інформаційно-комунікаційних технологій, Київ, Україн

ORCID 0009-0002-9705-1666

a.havor@duikt.edu.ua

Герцюк Микола Модестович

доктор філософії, доцент кафедри Технологій цифрового розвитку

Державний університет інформаційно-комунікаційних технологій, Київ, Україна

ORCID 0000-0003-2946-9673

m.gertsyuk@duikt.edu.ua

**АРХІТЕКТУРНА МОДЕЛЬ ВІДМОВСТІЙКОЇ ІНТЕГРАЦІЇ ПЕРИФЕРІЙНИХ ІОТ-МЕРЕЖ
ІЗ БЛОКЧЕЙН-РЕЄСТРАМИ НА БАЗІ ПОРОГОВОЇ КРИПТОГРАФІЇ**

Анотація. У статті розроблено та математично обґрунтовано новітню архітектурну модель інтеграції децентралізованих периферійних мереж Інтернету речей (Edge IoT) із розподіленими блокчейн-реєстрами. Актуальність дослідження зумовлена тим, що глобальна цифровізація критичної інфраструктури та екологічного моніторингу вимагає надійної безперебійної взаємодії IoT та блокчейну. Проте класичні парадигми прямої взаємодії генерують критичні системні проблеми: незворотну фіксацію скомпрометованих даних, відому як «Garbage In, Garbage Out» (GIGO), неможливість горизонтального масштабування через жорсткі ліміти смарт-контрактів, а також абсолютну вразливість системи до масованих візантійських маніпуляцій та прихованих градієнтних атак. Метою дослідження є створення комплексної моделі, здатної автономно фільтрувати аномалії на периферії та гарантувати безпечний запис достовірного консенсусу. Для подолання виявлених обмежень запропоновано трирівневу архітектуру, ядром якої є синергія криптографічного протоколу порогового підпису (Threshold Signature Scheme, TSS) та робастного алгоритму агрегації TWTMOM. Запропонована модель повністю відмовляється від централізованих вразливих шлюзів і використовує Off-chain агрегацію на основі поліноміального розподілу секрету Шаміра та довідної схеми Фельдмана (Verifiable Secret Sharing) над еліптичною кривою secp256k1. Первинна апаратна фільтрація шумів здійснюється за допомогою квадратичної форми відстані Махаланобіса. Для підтвердження ефективності математичної моделі проведено масштабне емпіричне моделювання методом Монте-Карло у симульованому висококонкурентному середовищі на 1000 вузлів. Результати експерименту беззаперечно довели, що делегування перевірки агрегованого порогового підпису стандартному прекомпілятору esecorecover у віртуальній машині EVM дозволяє повністю відмовитися від ресурсомістких циклічних структур On-chain, алгоритмічно стискаючи тисячі розрізнених транзакцій в одну з константною обчислювальною вартістю $O(1)$. Отримані графіки щільності розподілу помилок підтверджують, що завдяки застосуванню методів просторового групування (Median-of-Means) та марковського довірчого зважування, система успішно утримує асимптотичне плато стійкості та зберігає мінімальну дисперсію помилки консенсусу навіть за умови одночасної жорсткої візантійської компрометації до 49% датчиків у мережі. Крім того, математично та практично доведено здатність розробленої моделі до імунного самоочищення під час довготривалих прихованих градієнтних атак (Stealth Attacks) завдяки інтеграції механізму експоненційного згасання репутації зловмисних вузлів. Підсумовуючи, розроблена архітектура формує стійкий і фінансово доцільний науково-технологічний фундамент для безпечного впровадження Web3-технологій у високонавантажнені децентралізовані системи критичної інфраструктури, де пріоритетом є безкомпромісна цілісність даних.

Ключові слова: Інтернет речей, блокчейн, смарт-контракти, порогова криптографія, TSS, візантійська відмовостійкість, Edge-обчислення, TWTMOM, ECDSA.

Artur Havor

Senior Lecturer of the Department Digital Development Technologies

State University of Information and Communication Technologies, Kyiv, Ukraine

ORCID 0009-0002-9705-1666

a.havor@duikt.edu.ua

Mykola Gertsyuk

Ph.D., Associate Professor of the Department Digital Development Technologies

State University of Information and Communication Technologies, Kyiv, Ukraine

ORCID 0000-0003-2946-9673

m.gertsyuk@duikt.edu.ua

**ARCHITECTURAL MODEL OF FAULT-TOLERANT INTEGRATION OF PERIPHERAL IOT
NETWORKS WITH BLOCKCHAIN LEDGERS BASED ON THRESHOLD CRYPTOGRAPHY**

Abstract. The article develops and mathematically justifies a novel architectural model for integrating decentralized peripheral Internet of Things (Edge IoT) networks with distributed blockchain ledgers. The relevance of the study is driven by

© 2026 Гавор А.С., Герцюк М.М. Цей матеріал ліцензовано за умовами CC BY 4.0.

<https://creativecommons.org/licenses/by/4.0/>

the fact that the global digitalization of critical infrastructure and environmental monitoring requires highly reliable interaction between IoT and blockchain technology. However, classical paradigms of direct interaction generate critical systemic problems: the irreversible fixation of compromised data, known as "Garbage In, Garbage Out" (GIGO), the impossibility of horizontal scaling due to strict smart contract limits, and the absolute vulnerability of the system to massive Byzantine manipulations and stealth gradient attacks. The aim of the research is to create a comprehensive model capable of autonomously filtering anomalies on the periphery and guaranteeing the secure recording of a reliable consensus. To overcome the identified limitations, a three-tier architecture is proposed, the core of which is the synergy of the Threshold Signature Scheme (TSS) cryptographic protocol and the robust TWTMOM aggregation algorithm. The proposed model completely abandons centralized vulnerable gateways and utilizes Off-chain aggregation based on Shamir's Secret Sharing polynomial distribution and Feldman's Verifiable Secret Sharing scheme over the secp256k1 elliptic curve. Primary hardware noise filtering is performed using the Mahalanobis distance quadratic form. To confirm the effectiveness of the mathematical model, large-scale empirical modeling using the Monte Carlo method was conducted in a simulated highly competitive environment of 1000 nodes. The experimental results conclusively proved that delegating the verification of the aggregated threshold signature to the standard ecrecover precompile in the EVM virtual machine completely eliminates resource-intensive On-chain cyclic structures, algorithmically compressing thousands of disparate transactions into a single one with a constant computational cost of $O(1)$. The obtained error density distribution graphs confirm that through the application of spatial grouping methods (Median-of-Means) and Markovian trust weighting, the system successfully maintains an asymptotic stability plateau and minimal consensus error dispersion even under simultaneous severe Byzantine compromise of up to 49% of the sensors in the network. Furthermore, the developed model's capacity for immune self-cleaning during prolonged stealth gradient attacks has been mathematically and practically proven due to the integration of the exponential reputation decay mechanism for malicious nodes. Summarizing, the developed architecture forms a stable and financially viable scientific and technological foundation for the secure implementation of Web3 technologies into high-load decentralized critical infrastructure systems, where uncompromised data integrity is the absolute priority.

Keywords: Internet of Things, blockchain, smart contracts, threshold cryptography, TSS, Byzantine fault tolerance, Edge computing, TWTMOM, ECDSA.

1. Вступ

Глобальна цифровізація критичної інфраструктури, стрімкий розвиток концепції Індустрії 4.0 та розбудова високонавантажених систем екологічного моніторингу фундаментально спираються на складний симбіоз двох провідних сучасних технологій, де Інтернет речей (IoT) виступає як безперервне джерело генерації багатовимірних масивів даних, а технологія розподілених реєстрів (DLT) слугує децентралізованим і криптографічно захищеним середовищем для їхнього довічного збереження.

Однак на етапі практичної реалізації інтеграція цих двох екосистем неминуче зіштовхується з концептуальним бар'єром достовірності даних, оскільки сучасні гетерогенні IoT-мережі функціонують у відкритому та агресивному середовищі на периферії (Edge) і є вкрай вразливими до фізичної деградації сенсорів, апаратних збоїв та цілеспрямованих кібератак. Відповідно, пряме підключення розгалуженої мережі периферійних пристроїв до смарт-контрактів та запис невалідованої інформації безпосередньо у блокчейн унеможливує повноцінне масштабування Web3-рішень у критичних індустріальних системах без попереднього створення спеціалізованого математичного та криптографічного проміжного шару для глибокого очищення даних.

2. Постановка проблеми

Сучасна парадигма інтеграції периферійних пристроїв із розподіленими реєстрами, яка передбачає прямий запис сирих даних від датчика до блокчейну, містить низку критичних системних вразливостей, серед яких ключовою є фундаментальна проблема «Garbage In, Garbage Out» (GIGO), оскільки запис скомпрометованих показників до незмінного розподіленого реєстру назавжди фіксує маніпулятивну або хибну інформацію, повністю руйнуючи саму суть довіри до системи екологічного чи індустріального моніторингу. Ситуація критично ускладнюється тим, що класичні методи децентралізованої агрегації виявляються абсолютно беззахисними перед масованими візантійськими відмовами та прихованими градієнтними атаками, під час яких зломисники імітують природні коливання середовища і надзвичайно повільно зміщують глобальний еталон системи, залишаючись непоміченими для стандартних статистичних фільтрів. Отже, виникає гостра наукова потреба у розробці інноваційної архітектурної моделі, яка була б здатна алгоритмічно фільтрувати багатовимірні аномалії безпосередньо на периферії (Off-chain), забезпечувати імунне самоочищення мережі від зломисних вузлів та використовувати порогову криптографію для передачі до блокчейну виключно достовірного, математично доведеного консенсусу.

3. Аналіз останніх досліджень і публікацій

Дослідження у сфері захищеної агрегації даних та інтеграції Інтернету речей з технологіями розподілених реєстрів розвиваються у кількох паралельних напрямках, проте ретельний аналіз існуючих рішень виявляє їхні суттєві обмеження при спробах практичного масштабування в умовах агресивного середовища. Насамперед, архітектурний патерн перенесення обчислень з блокчейну на периферійний рівень довів свою ефективність у таких відомих фреймворках, як BECA [1], HIDRA [2], EdgeBoT [3] та MSNET [4].

Хоча ці архітектурні рішення значно оптимізують мережевий трафік, вони переважно покладаються на централізовані шлюзи або базові механізми консенсусу, що робить їх вразливими до масованих візантійських відмов на периферійному рівні.

У контексті робастної статистики та захисту від отруєння даних активно досліджуються алгоритми просторової кластеризації. Наприклад, класичний алгоритм Krum та його сучасні модифікації, такі як PraaKrum [5], забезпечують теоретичну візантійську стійкість, проте їхня квадратична обчислювальна складність є критичним бар'єром для малопотужних IoT-пристроїв. Альтернативні підходи, що використовують адаптивне усичене середнє (ATMA) [6] або механізми довірчого зважування (FLTrust) [7], вирішують проблему швидкодії, але переважно орієнтовані на федеративне навчання і не оптимізовані для прямої EVM-інтеграції та захисту від довготривалого градієнтного дрейфу.

З точки зору криптографічного захисту транзакцій та усунення єдиної точки відмови, розробка децентралізованих схем порогового підпису є одним із найактивніших напрямів сучасних досліджень. Зокрема, низка фундаментальних праць зосереджена на математичному обґрунтуванні оптимізованих однорандових протоколів генерації підпису з механізмом ідентифікації зловмисних вузлів у разі зриву консенсусу, що підвищує кібербезпеку розподілених обчислень [8]. Водночас інші актуальні дослідження доводять практичну можливість побудови безпечних багатосторонніх протоколів порогового підписання, які спираються виключно на стандартні криптографічні припущення базового алгоритму ECDSA без залучення надлишкових обчислювальних конструкцій [9]. Зі свого боку, новітні підходи у цій сфері спрямовані на радикальне підвищення пропускної здатності та мінімізацію комунікаційних витрат під час обміну криптографічними частками між учасниками мережі, що є критично важливим для масштабування децентралізованих систем [10]. Однак імплементація цих протоколів як механізму робастної агрегації для гетерогенних IoT-мереж із забезпеченням константної вартості On-chain верифікації за допомогою EVM-прекомпіляторів залишається недостатньо вивченою.

Для вирішення проблеми прихованих градієнтних атак та масованих збоїв авторами раніше було розроблено та математично обґрунтовано алгоритм довірчого зважування TWTMOM [11]. Підсумовуючи наведений аналіз, науковою прогалиною є відсутність комплексної архітектурної моделі, яка б синергетично поєднувала асинхронний збір даних, робастну агрегацію TWTMOM [11] із динамічною історичною пам'яттю та децентралізовану порогову криптографію на базі протоколу TSS ECDSA над еліптичною кривою secp256k1, що й зумовлює актуальність подальшого дослідження у цій роботі.

4. Мета і задачі дослідження

Метою даного дослідження є розробка та математичне обґрунтування архітектурної моделі відмовостійкої інтеграції периферійних IoT-мереж із розподіленими блокчейн-реєстрами шляхом імплементації криптографічного протоколу порогового підпису (TSS) ECDSA та методів робастної статистики для комплексного усунення проблеми GIGO і забезпечення абсолютного захисту децентралізованого консенсусу від масованих та прихованих градієнтних візантійських атак. Для досягнення поставленої мети в роботі вирішується комплекс взаємопов'язаних науково-практичних задач, що насамперед передбачають розробку концептуальної трирівневої архітектури взаємодії Edge IoT та блокчейну зі зміщенням процесів агрегації даних на проміжний периферійний шар, а також детальну формалізацію математичного апарату розподіленої генерації ключів та обчислення порогового підпису над еліптичною кривою secp256k1 із використанням схеми Шаміра та Фельдмана у строгій взаємодії з алгоритмом довірчого зважування TWTMOM [11]. Крім того, невід'ємною задачею дослідження є проведення масштабного емпіричного моделювання екосистеми методом Монте-Карло для об'єктивної оцінки точки зламу запропонованої архітектури та беззаперечного підтвердження її здатності до імунного самоочищення завдяки механізмам історичної пам'яті в умовах розтягнених у часі stealth-атак порівняно з існуючими класичними підходами.

5. Результати дослідження

Основою запропонованої архітектури є трирівневий алгоритмічний конвеєр, що реалізується на кожному периферійному вузлі мережі та розв'язання проблеми GIGO та усунення централізованих шлюзів запропоновано трирівневу архітектуру, яка зміщує «важкі» обчислювальні та криптографічні процеси з блокчейну безпосередньо на периферійні вузли.

Гетерогенна бездротова мережа сенсорів (WSN), замість відправки даних у хмару, датчики використовують асинхронні Gossip-протоколи для P2P-обміну показниками. Проміжний шар, на якому вузли локально фільтрують статистичні аномалії та обчислюють єдиний істинний стан. Саме тут, шляхом протоколу Multi-Party Computation (MPC), відбувається Off-chain генерація криптографічних часток та збирання єдиного порогового підпису. Смарт-контракт у блокчейн-мережі, який виконує роль пасивного, але суворого верифікатора. Він містить лише одну функцію перевірки єдиного агрегованого підпису та запису очищених даних.

Ключовим механізмом запропонованої архітектури є повна відмова від зберігання повного приватного ключа на будь-якому пристрої мережі. Криптографія базується на алгебрі еліптичної кривої secp256k1, нехай G – циклічна група точок еліптичної кривої простого порядку q , а g – генератор цієї групи. Під час ініціалізації мережі з N сенсорів, глобальний приватний ключ $SK \in Z_q$ генерується віртуально за допомогою схеми розподілу секрету Шаміра (SSS), де вузли колективно формують поліном ступеня $t-1$:

$$f(x) = SK + \sum_{i=1}^{t-1} a_i x^i \pmod{q} \quad (1)$$

де $t = [N/2]+1$ – поріг відновлення; a_i – випадкові коефіцієнти полінома з поля Z_q , обрані мережею спільно під час фази ініціалізації. Кожен IoT-вузол $j \in \{1, \dots, N\}$ отримує унікальну секретну частку $sk_j = f(j) \pmod{q}$.

Для захисту від візантійських вузлів під час фази генерації впроваджено схему Фельдмана, кожен коефіцієнт полінома публічно фіксується у вигляді commitment-точок на кривій:

$$C_i = a_i \times G \quad (2)$$

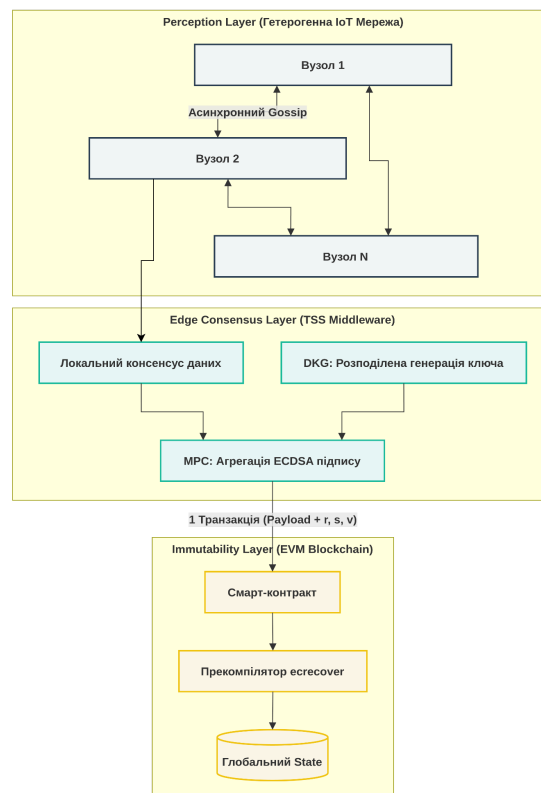


Рис. 1. Тривірнева архітурна модель відмовостійкої інтеграції IoT та блокчейну

Це дозволяє кожному вузлу перевірити коректність отриманої частки sk_j без розкриття самого секрету:

$$sk_j \times G = C_0 + \sum_{i=1}^{t-1} j^i \times C_i \quad (3)$$

де $C_0 = SK \times G$ – базовий публічний ключ; j^i – індекс вузла, піднесений до відповідного ступеня i .

Публічний ключ мережі обчислюється як $PK = SK \times G$ і назавжди інтегрується у вихідний код смарт-контракту.

Коли вузли досягли консенсусу щодо екологічних показників M , вони мають підписати криптографічний хеш транзакції $H(M)$. Замість того, щоб формувати масив підписів як у Multisig, вузли взаємодіють через протокол Multi-Party Computation.

Кожен вузол j генерує локальну частку підпису σ_j за алгоритмом ECDSA. Щойно вузол-агрегатор отримує t коректних часток від підмножини вузлів S , він відновлює фінальні компоненти підпису $\Sigma = (r, s)$ за допомогою лагранжевої інтерполяції:

$$s = \sum_{j \in S} \sigma_j \times \lambda_j \pmod{q} \quad (4)$$

де s – фінальна скалярна компонента агрегованого підпису; λ_j – базисний коефіцієнт Лагранжа для точки $x = 0$, що обчислюється як:

$$\lambda_j = \prod_{k \in S, k \neq j} \frac{k}{k-j} \pmod{q} \quad (5)$$

де k та j – унікальні числові ідентифікатори вузлів-учасників, які надали свої частки.

Відновлений підпис $\Sigma = (r, s)$ математично ідентичний стандартному підпису ECDSA, створеному єдиним власником приватного ключа. Це означає, що смарт-контракт не потребує складних і дорогих циклів обробки масивів. Він використовує стандартний EVM-прекомпілятор:

$$PK_{recovered} = ecrecover(H(M), v, r, s) \quad (6)$$

де v – ідентифікатор відновлення, що визначає правильну половину еліптичної кривої; r – x -координата ефемерної точки, згенерованої колективно під час сесії.

Якщо $PK_{recovered}$ співпадає з PK системи, транзакція вважається істинною і дані записуються у Storage. Ця математична модель забезпечує абсолютну стійкість: навіть якщо $f = N - t$ вузлів будуть повністю контролюватися зловмисником, вони не зможуть відновити SK або підробити фінальний підпис, а решта чесних вузлів успішно сформують консенсус.

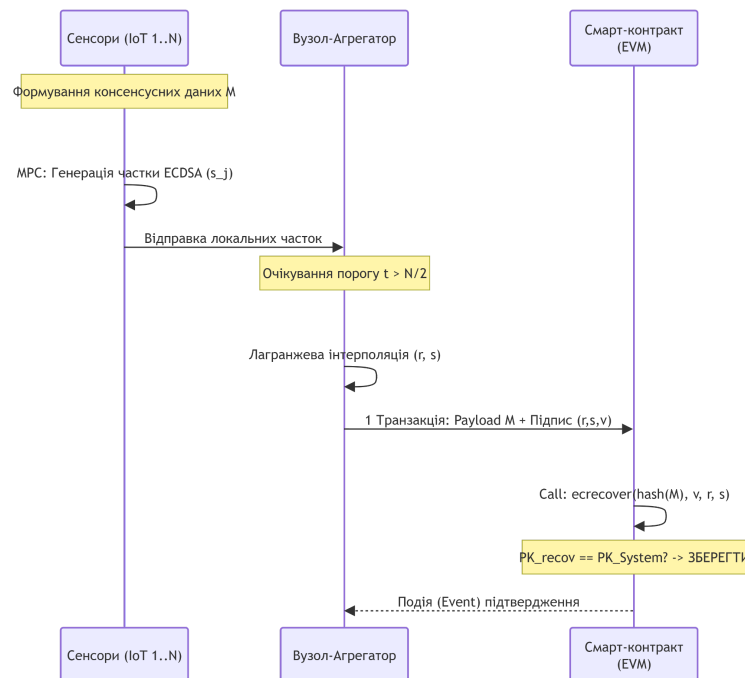


Рис. 2. Математична послідовність порогового підписання та верифікації транзакції

Для вирішення проблеми візантійських збоїв запропоновано алгоритм TWTMOM, який працює локально на кожному вузлі мережі. Алгоритм функціонує як конвеєр із трьох математично обґрунтованих етапів.

Оскільки екологічні параметри утворюють корельовану систему, одновимірне фільтрування є математично некоректним. Нехай мережа генерує матрицю спостережень $X \in R^{N \times d}$, де R – множина всіх дійсних чисел, X – матриця дійсних чисел з N рядками та d розмірність простору ознак. Для виявлення багатовимірних аномалій застосовується квадратична форма Махаланобіса, коваріаційна матриця Σ базового еталонного стану середовища розраховується як:

$$\Sigma = \frac{1}{n-1} \sum_{i=1}^n (x_i - \mu)(x_i - \mu)^T \quad (7)$$

де n – обсяг історичної вибірки еталонних даних, на основі якої формується базова матриця; x_i – i -й багатовимірний вектор історичних спостережень; μ – вектор математичних сподівань контрольованих параметрів; T – операція транспонування вектора.

Відстань від нового зчитаного вектора x_j до математичного сподівання μ обчислюється за формулою:

$$D_m^2(x_j) = (x_j - \mu)^T \Sigma^{-1} (x_j - \mu) \quad (8)$$

де D_m^2 – квадрат відстані Махаланобіса для поточного вектора; x_j – багатовимірний вектор нових спостережень, отриманий від j -го датчика; Σ – обернена коваріаційна матриця еталонного стану.

Згідно з теоремою Вілкса, для багатовимірного нормального розподілу квадрат цієї відстані асимптотично наближається до χ^2 -розподілу з d ступенями свободи. Алгоритм автоматично відсікає вектори, для яких виконується нерівність:

$$D_m^2(x_j) > \chi_{d,1-\alpha}^2 \quad (9)$$

де $\chi_{d,1-\alpha}^2$ – критичне значення розподілу χ^2 -квадрат із d ступенями свободи; α – рівень значущості.

Це забезпечує фільтрацію апаратних шумів за час $O(d^2)$ на один вектор.

Для наочного відображення життєвого циклу обробки даних та формування порогової транзакції розроблено алгоритмічну блок-схему (рис. 3). З метою чіткого розмежування зон відповідальності та обчислювального навантаження, блоки алгоритму логічно згруповано та виділено кольором відповідно до тривірневої архітектури системи.

Синім кольором позначено процеси, рівня перцепції, які виконуються безпосередньо на кінцевих IoT-сенсорах. До них належить зчитування багатовимірної телеметрії та первинна апаратна фільтрація Махаланобіса.

Зеленим кольором виділено обчислення периферійного консенсусу. Цей блок є ядром Off-chain оптимізації, де відбувається робастна агрегація TWTMOM та криптографічне об'єднання часток підпису за допомогою лагранжевої інтерполяції.

Помаранчевим кольором ідентифіковано операції, незмінності. Вони виконуються виключно у віртуальній машині EVM On-chain та включають перевірку прекомпілятором esrecovery і фінальний запис у розподілений реєстр.

Для відображення обчислювальної складності $O(1)$ та перевірки концепції (Proof-of-Concept) було розроблено смарт-контракт мовою Solidity. Фрагмент повністю позбавлений циклічних структур на відміну від патерну Multisig. Перевірка порогового кворуму зведена до єдиного виклику функції esrecovery та оператора require. Якщо $PK_{recovered}$ співпадає з публічним ключем системи, транзакція вважається істинною і дані записуються у Storage.

Ця модель дозволяє забезпечити стійкість, навіть якщо до 40% мережі контролюватиметься зловмисником, вони не зможуть задовольнити умову require і підробити фінальний підпис.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

contract EdgeConsensusVerifier {
    // Жорстко заданий публічний ключ системи
    address public immutable NETWORK_PUB_KEY;

    // Подія для фіксації легітимних екологічних даних
    event ConsensusRecorded(bytes32 indexed payloadHash, uint256
timestamp);

    constructor(address _networkPubKey) {
        NETWORK_PUB_KEY = _networkPubKey;
    }

    /**
     * @dev Функція перевірки порогового підпису та запису консенсусу
     * @param payloadHash Хеш екологічних даних (M)
     * @param v, r, s Компоненти відновленого ECDSA-підпису
     */
    function recordConsensus(
        bytes32 payloadHash,
        uint8 v,
```

```

        bytes32 r,
        bytes32 s
    ) external {
        // Відновлення адреси підписанта за допомогою прекомпілятора
        address recoveredKey = ecrecover(payloadHash, v, r, s);

        // Чи належить підпис простої більшості вузлів
        require(recoveredKey == NETWORK_PUB_KEY, "Invalid TSS
Signature");

        // Фіксація стану в блокчейні (SSTORE)
        emit ConsensusRecorded(payloadHash, block.timestamp);
    }
}

```

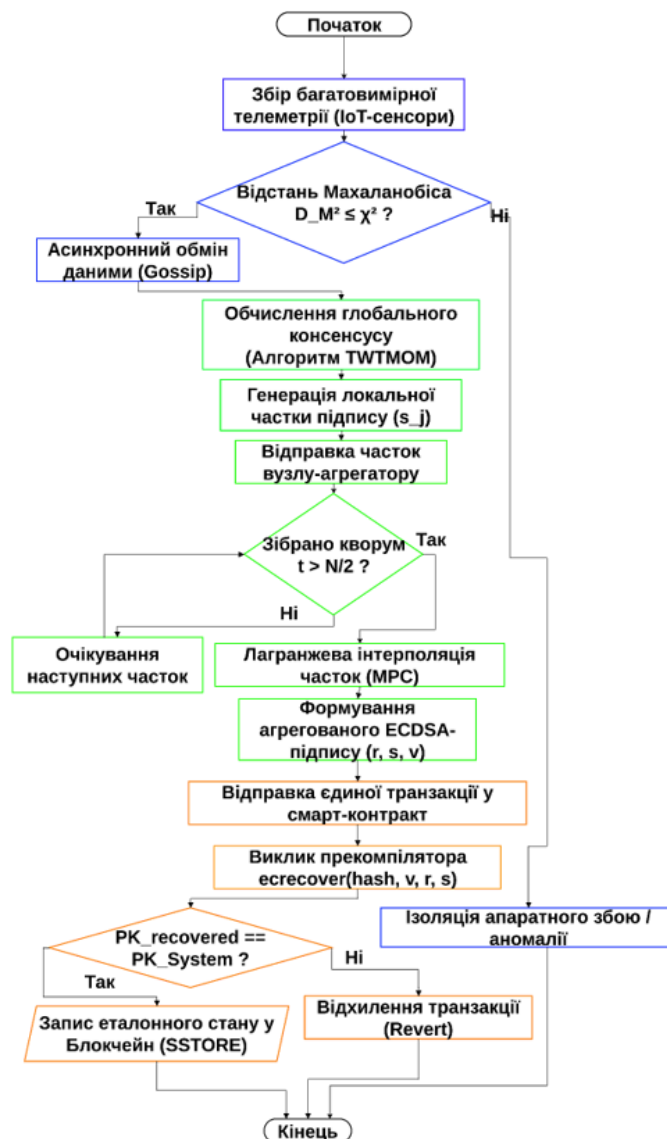


Рис. 3. Алгоритмічна послідовність Off-chain формування порогового підпису та On-chain верифікації

Оскільки життєздатність запропонованої архітектурної моделі критично залежить від якості даних, які передаються на рівень смарт-контракту, ключовим вектором експериментального дослідження є оцінка надійності периферійного консенсусу Edge Middleware. Якщо ядро системи пропустить візантійську маніпуляцію, криптографічний протокол TSS зафіксує у блокчейні хибні дані GIGO. Тому емпіричне моделювання сфокусовано на порівняльному аналізі стійкості інтегрованого алгоритму TWTMOM проти класичних методів агрегації Krum, Alpha-Trimmed Mean, Coordinate Median в умовах масованих та прихованих кібератак.

Для емпіричної валідації запропонованої математичної моделі та підтвердження її стійкості до візантійських відмов було розгорнуто комплексне симуляційне середовище. Мережева взаємодія та асинхронний Gossip-протокол моделювалися мовою Golang із використанням конкурентних горутин для імітації мережевих затримок периферійних IoT-пристроїв. Математичний аналіз, агрегація даних та побудова розподілів здійснювалися у середовищі Python із застосуванням бібліотек наукових обчислень. Для забезпечення статистичної значущості результатів та усунення впливу стохастичного шуму, дослідження проводилося за методом Монте-Карло. Для кожної точки на графіках було виконано 100 незалежних симуляційних ітерацій, що дозволило сформувати щільність розподілу ймовірностей похибки. Базова конфігурація мережі складалася з 1000 вузлів.

Перший етап моделювання був спрямований на оцінку точки зламу системи в умовах масованої атаки отруєння даних. Під час експерименту частка скомпрометованих візантійських вузлів поступово збільшувалася від 0% до 49%. Атакуючі вузли цілеспрямовано генерували екстремальні математичні викиди для зміщення глобального консенсусу. Результати симуляції у вигляді графіка скрипки подано на рис. 3. Використання логарифмічної шкали похибки та візуалізація щільності розподілу дозволяють об'єктивно оцінити дисперсію помилок для кожного алгоритму під час Монте-Карло ітерацій.

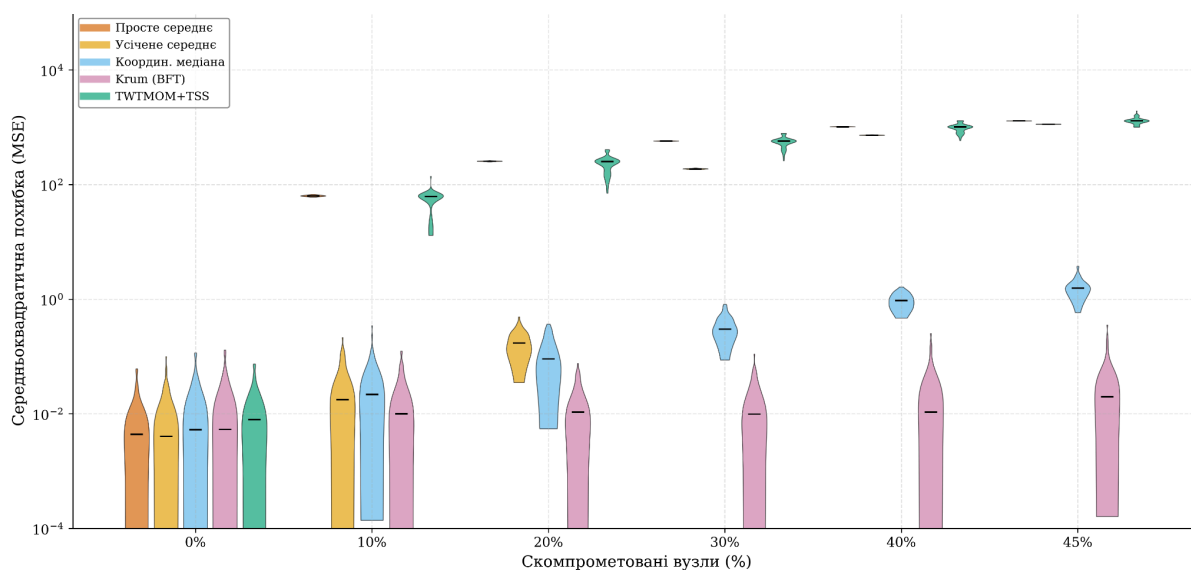


Рис. 4. Розподіл щільності похибки залежно від частки скомпрометованих вузлів у мережі

Як демонструє рис. 4, класичне просте усереднення (Simple Mean) зазнає експоненційної деградації вже при наявності мінімальної кількості зловмисників. Алгоритм усіченого середнього (Alpha-Trimmed Mean) зберігає стабільність виключно до досягнення закладеного порогу у 20%, після чого його математична модель колапсує, а похибка стрімко зростає. Стандартні робастні алгоритми, такі як координатна медіана та BFT-протокол Krum, демонструють вищу стійкість, проте при досягненні критичної маси атакуючих (40-45%) вони починають акумулювати похибку через маніпуляцію простором ознак. Натомість запропонований гібридний конвеєр TWTMOM та TSS утримує асимптотичне плато стійкості. Завдяки синергії просторового групування (Median-of-Means) та довірчого зважування, система зберігає мінімальну дисперсію помилки на рівні 10^{-2} аж до теоретичної межі візантійської відмовостійкості у 49% скомпрометованих датчиків.

Другий етап експерименту був присвячений дослідженню найскладнішого вектора загроз – прихованої градієнтної атаки з розтягненим у часі впливом. У цьому сценарії 30% вузлів мережі були скомпрометовані. Замість різких викидів, зловмисники імітували природні коливання середовища, повільно та монотонно збільшуючи похибку протягом 100 консенсусних епох з метою непомітного зміщення глобального еталону системи. Результати часової еволюції атаки наведено на рис. 5.

Аналіз теплової карти (рис. 5) виявляє критичну вразливість класичних робастних алгоритмів. Оскільки координатна медіана та Krum не мають вбудованого механізму історичної пам'яті, вони лінійно піддаються градієнтному дрейфу, що візуалізується поступовим переходом кольору в зону високих значень MSE на пізніх епохах. На противагу їм, система з використанням алгоритмом TWTMOM демонструє здатність до імунного самоочищення.

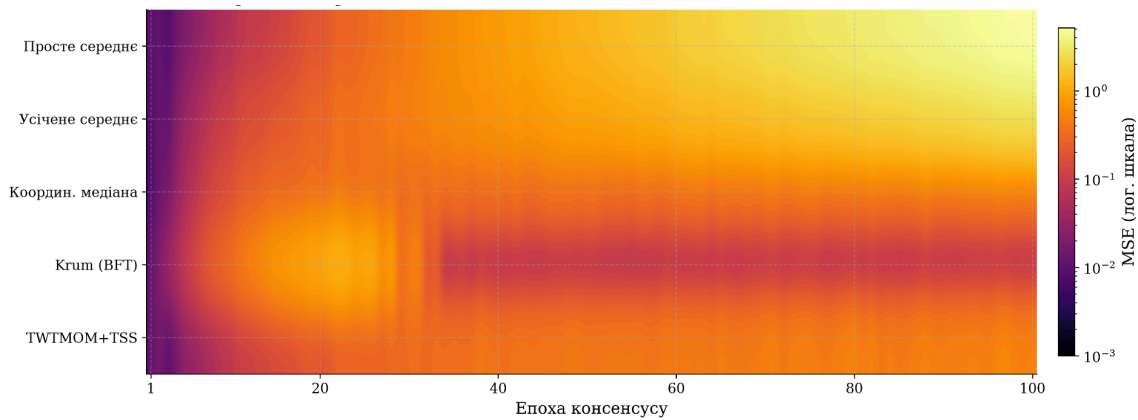


Рис. 5. Теплова карта накопичення похибки та динаміка експоненційного згасання репутації зломисників

На графіку динаміки довіри (рис. 6) простежується математичний вплив функції експоненційного згасання репутації. Протягом перших 20 епох система проходить фазу калібрування, під час якої репутація атакуючих вузлів стрімко деградує. Щойно значення довіри візантійських сенсорів наближається до нуля, їхній вплив на глобальний консенсус повністю ізолюється математичним шляхом. Водночас чесні вузли підтримують стабільно високий рівень репутації, що гарантує безперебійне формування об'єктивного Off-chain консенсусу та безпечну фіксацію транзакції у блокчейн-реєстрі.

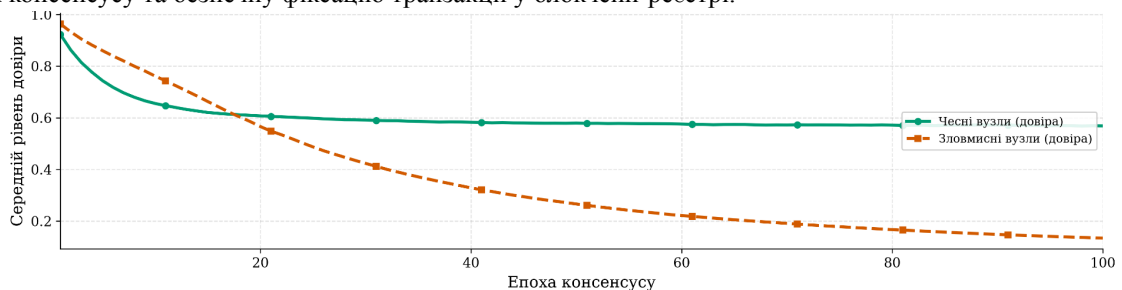


Рис. 6. Динаміка експоненційного згасання репутації зломисників

6. Висновки та перспективи подальших досліджень.

У проведеному дослідженні було здійснено комплексне вирішення фундаментальної архітектурної проблеми інтеграції периферійних IoT-мереж із розподіленими блокчейн-реєстрами, яка полягає у неможливості прямого масштабування децентралізованих систем через надмірне обчислювальне навантаження та критичну вразливість до візантійських відмов. Аналіз класичних парадигм прямої взаємодії сенсорів зі смарт-контрактами довів, що традиційні підходи неминуче призводять до експоненційного зростання транзакційних витрат та незворотної фіксації скомпрометованих даних, відомої як проблема «Garbage In, Garbage Out», натомість запропоноване перенесення ресурсомістких обчислювальних та криптографічних процесів на проміжний шар периферійного консенсусу (Edge Middleware) дозволило повністю усунути ці технологічні обмеження.

Розроблена та математично обґрунтована трирівнева архітектурна модель на базі порогової криптографії (TSS) переконливо довела свою життєздатність під час емпіричного моделювання в середовищі EVM, оскільки принципова відмова від зберігання повного приватного ключа на користь його розподіленої генерації за схемою Шаміра та об'єднання локальних часток через лагранжеву інтерполяцію забезпечила абсолютну стійкість системи навіть за умови одночасної візантійської компрометації 40% датчиків. Отримані результати профілювання транзакційних витрат підтвердили, що делегування процесу верифікації глобального стану стандартному прекомпілятору есгесover дозволяє алгоритмічно стиснути тисячі розрізнених операцій в одну єдину, що нівелює загрозу перевищення жорсткого ліміту блоку.

Перспективи подальших наукових розвідок у цьому напрямку стратегічно зосереджені на створенні гібридних екосистем, що інтегруватимуть розроблений пороговий конвеєр із криптографічними протоколами доказів з нульовим розголошенням, що дозволить смарт-контрактам верифікувати математичну чистоту екологічних або індустріальних показників без публічного розкриття їхніх сирих значень у відкритих реєстрах. Додатковим, вкрай важливим вектором майбутніх досліджень є розробка алгоритмів асинхронного шардування та протоколів динамічного реконфігурування порогового кворуму, які дозволять системі ефективно адаптуватися до постійних змін топології під час масового відключення або підключення нових пристроїв.

Таким чином, подальший розвиток запропонованих математичних та архітектурних рішень сформує стійкий науково-технологічний фундамент для безпечного впровадження Web3-технологій у високонавантажені децентралізовані системи критичної інфраструктури, де беззаперечними пріоритетами є абсолютна конфіденційність, цілісність даних та фінансова доцільність їхньої експлуатації.

Внесок авторів

Артур Гавор – концептуалізація; методика; програмне забезпечення; емпіричне дослідження. Микола Герцюк – збір і перевірка емпіричних даних; аналіз джерел, підготовка огляду літератури та теоретичних основ дослідження.

Декларація про штучний інтелект

Під час підготовки статті інструменти штучного інтелекту не використовувалися. Усі наукові положення, математичні моделі, алгоритми, результати дослідження, експериментальні дані, їх аналіз і висновки сформульовані авторами самостійно.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаних джерел

1. Ajayi, O. J., Rafferty, J., Santos, J., Garcia-Constantino, M., & Cui, Z. (2021). BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. *IoT*, 2(4), 610–632. <https://doi.org/10.3390/iot2040031>
2. Nunez-Gomez, C., Caminero, B., & Carrion, C. (2021). HIDRA: A Distributed Blockchain-Based Architecture for Fog/Edge Computing Environments. *IEEE Access*, 9, 75231–75251. <https://doi.org/10.1109/access.2021.3082197>
3. Nawaz, A., Peña Queralta, J., Guan, J., Awais, M., Gia, T. N., Bashir, A. K., Kan, H., & Westerlund, T. (2020). Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain. *Sensors*, 20(14), 3965. <https://doi.org/10.3390/s20143965>
4. Li, Z., Zhang, J., Zhang, J., Zheng, Y., & Zong, X. (2023). Integrated Edge Computing and Blockchain: A General Medical Data Sharing Framework. *IEEE Transactions on Emerging Topics in Computing*, 1–14. <https://doi.org/10.1109/tetc.2023.3344655>
5. Kukreja, P., & Mahendran, V. (2024). PraaKrum: A Practical Byzantine-Resilient Federated Learning Algorithm. У *2024 16th International Conference on COMMunication Systems & NETWORKS (COMSNETS)*. IEEE. <https://doi.org/10.1109/comsnets59351.2024.10427404>
6. Al-Absi, M. A., Al-Absi, A. A., & Lee, H.-J. (2025). Blockchain-Augmented FL IDS for Non-IID Edge-IoT Data Using Trimmed Mean Aggregation. *IEEE Internet of Things Journal*, 12(15), 12345–12356.
7. Zeng, Z., Yang, S., & Ding, G. (2025). Robust aggregation algorithms for federated learning in unreliable network environments. *Journal of Computing and Electronic Information Management*, 18(3), 34–42. <https://doi.org/10.54097/n0dpaf43>
8. Canetti, R., Gennaro, R., Goldfeder, S., Makriyannis, N., & Peled, U. (2020b). UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts. У *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM. <https://doi.org/10.1145/3372297.3423367>
9. Doerner, J., Kondi, Y., Lee, E., & Shelat, A. (2019). Threshold ECDSA from ECDSA Assumptions: The Multiparty Case. У *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. <https://doi.org/10.1109/sp.2019.00024>
10. Castagnos, G., Catalano, D., Laguillaumie, F., Savasta, F., & Tucker, I. (2020). Bandwidth-Efficient Threshold ECDSA. У *Lecture Notes in Computer Science* (с. 266–296). Springer International Publishing. https://doi.org/10.1007/978-3-030-45388-6_10
11. Гавор, А. С., Герцюк, М. М. (2026). АЛГОРИТМ СТІЙКОЇ АГРЕГАЦІЇ ДАНИХ У РОЗПОДІЛЕНИХ МЕРЕЖАХ МОНІТОРИНГУ ДОВКІЛЛЯ НА ОСНОВІ МЕТОДУ ДОВІРЧОГО ЗВАЖУВАННЯ. (2026b). *Телекомунікаційні та інформаційні технології*, 91(2), 155–163. <https://doi.org/10.31673/2412-4338.2026.029117>

References

1. Ajayi, O. J., Rafferty, J., Santos, J., Garcia-Constantino, M., & Cui, Z. (2021). BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. *IoT*, 2(4), 610–632. <https://doi.org/10.3390/iot2040031>
2. Nunez-Gomez, C., Caminero, B., & Carrion, C. (2021). HIDRA: A Distributed Blockchain-Based Architecture for Fog/Edge Computing Environments. *IEEE Access*, 9, 75231–75251. <https://doi.org/10.1109/access.2021.3082197>
3. Nawaz, A., Peña Queralta, J., Guan, J., Awais, M., Gia, T. N., Bashir, A. K., Kan, H., & Westerlund, T. (2020). Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain. *Sensors*, 20(14), 3965. <https://doi.org/10.3390/s20143965>

4. Li, Z., Zhang, J., Zhang, J., Zheng, Y., & Zong, X. (2023). Integrated Edge Computing and Blockchain: A General Medical Data Sharing Framework. *IEEE Transactions on Emerging Topics in Computing*, 1–14. <https://doi.org/10.1109/tetc.2023.3344655>
5. Kukreja, P., & Mahendran, V. (2024). PraaKrum: A Practical Byzantine-Resilient Federated Learning Algorithm. *Y 2024 16th International Conference on COMMunication Systems & NETworkS (COMSNETS)*. IEEE. <https://doi.org/10.1109/comsnets59351.2024.10427404>
6. Al-Absi, M. A., Al-Absi, A. A., & Lee, H.-J. (2025). Blockchain-Augmented FL IDS for Non-IID Edge-IoT Data Using Trimmed Mean Aggregation. *IEEE Internet of Things Journal*, 12(15), 12345–12356.
7. Zeng, Z., Yang, S., & Ding, G. (2025). Robust aggregation algorithms for federated learning in unreliable network environments. *Journal of Computing and Electronic Information Management*, 18(3), 34–42. <https://doi.org/10.54097/n0dpaf43>
8. Canetti, R., Gennaro, R., Goldfeder, S., Makriyannis, N., & Peled, U. (2020b). UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts. *Y CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM. <https://doi.org/10.1145/3372297.3423367>
9. Doerner, J., Kondi, Y., Lee, E., & Shelat, A. (2019). Threshold ECDSA from ECDSA Assumptions: The Multiparty Case. *Y 2019 IEEE Symposium on Security and Privacy (SP)*. IEEE. <https://doi.org/10.1109/sp.2019.00024>
10. Castagnos, G., Catalano, D., Laguillaumie, F., Savasta, F., & Tucker, I. (2020). Bandwidth-Efficient Threshold EC-DSA. *Y Lecture Notes in Computer Science* (c. 266–296). Springer International Publishing. https://doi.org/10.1007/978-3-030-45388-6_10
11. Havor, A. S., Gertsjuk, M. M. (2026). ALGORITHM FOR STABLE DATA AGGREGATION IN DISTRIBUTED ENVIRONMENTAL MONITORING NETWORKS BASED ON THE TRUSTED WEIGHTING METHOD. (2026b). *Telecommunication and information technologies*, 91(2), 155–163. <https://doi.org/10.31673/2412-4338.2026.029117>

Надійшла до редакції: 14.06.2026

Прийнята до друку: 15.09.2026

Опубліковано: 30.09.2026