№ 5(46) 2025
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.056.55+004.738.5+004.658

https://doi.org/10.52058/2786-6025-2025-5(46)-1835-1847

Нежуренко Олександр Григорович кандидат технічних наук, старший викладач кафедри комп'ютерних наук та інформаційних технологій, Житомирський державний університет імені Івана Франка, https://orcid.org/0009-0007-4594-9606

ЕФЕКТИВНІСТЬ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ МЕРЕЖЕВОГО ТРАФІКУ

Анотація. Стаття присвячена огляду криптографічних стратегій і алгоритмів консенсусу (PoW, PoS, PBFT), тестуванню їх масштабованості, енергоспоживання і затримок, а також їх використанню в мережах Інтернету речей. Масштабованість, квантова стійкість і конфіденційність є основними проблемами, що розглядаються в цій роботі, оскільки рішення, засновані на інтеграції 5G і ШІ, спрямовані на вирішення цих проблем і поліпшення систем безпеки.

Мета статті. Метою дослідження є аналіз технічної ефективності блокчейн-технологій для забезпечення безпеки мережевого трафіку.

Наукова новизна. Дослідження пропонує комплексний аналіз блокчейн-технологій як інструменту захисту мережевого трафіку, акцентуючи на порівнянні продуктивності алгоритмів консенсусу (PoW, PoS, PBFT) у реальних сценаріях, включаючи IoT. Новизна полягає у вивченні інтеграції блокчейну з AI та 5G для підвищення ефективності обробки трафіку, а також у розробці підходів до вирішення проблем масштабованості та квантової стійкості. Запропоновано використання гібридних консенсусних механізмів (PoS+BFT) та квантово-стійких алгоритмів (LMS, XMSS), що забезпечують адаптацію до сучасних викликів кібербезпеки.

Результати. Блокчейн забезпечує захист мережевого трафіку через децентралізацію, усуваючи єдину точку відмови. Криптографічні механізми, такі як хеш-функції SHA-256 і цифрові підписи ECDSA, гарантують цілісність і автентичність даних, знижуючи ризик маніпуляцій до 0,01%. Алгоритм PoS підвищує пропускну здатність до 100 транзакцій/с і знижує енергоспоживання до 0,01 кВт·год порівняно з PoW (700 кВт·год/транзакцію). PBFT забезпечує затримку менше 100 мс у мережах до 100 вузлів. У IoT-мережах блокчейн знижує ризик атак на 90% за допомогою протоколу LEACH, оптимізуючи енергоспоживання на 15–20%. Смарт-контракти та zk-SNARKs підвищують конфіденційність і швидкість реакції на аномалії (50–100 мс). Інтеграція з AI дозволяє виявляти аномалії з точністю 95%, а 5G знижує затримку до 5 мс, забезпечуючи пропускну здатність до 1000 транзакцій/с.

Висновки. Блокчейн-технології ефективно захищають мережевий трафік завдяки незмінності, децентралізації та криптографічним механізмам, знижуючи ризик атак, зокрема DDoS, при навантаженні до 10^6 запитів/с. PoS і PBFT оптимізують продуктивність, а LEACH зменшує енергоспоживання в IoT. Обмеження масштабованості та квантової стійкості вирішуються гібридними консенсусами та квантово-стійкими алгоритмами. Інтеграція з AI та 5G забезпечує аналіз у реальному часі та високу пропускну здатність. Подальші дослідження мають зосередитися на вдосконаленні консенсусних механізмів і квантово-стійкої криптографії для довгострокового захисту мереж.

Ключові слова: інформаційна безпека, блокчейн, кібербезпека, передача даних, захист даних.

Nezhurenko Oleksandr Phd in Technical Sciences, Senior Lecturer Department of Computer Science and Information Technology, Zhytomyr Ivan Franko State University, https://orcid.org/0009-0007-4594-9606

EFFICIENCY OF BLOCKCHAIN TECHNOLOGIES IN ENSURING THE SECURITY OF NETWORK TRAFFIC

Abstract. The piece is centered on reviewing cryptographic strategies and consensus algorithms (PoW, PoS, PBFT), testing their scalability, energy use and latency, as well as using them in Internet of Things networks. Scalability, the stability of quantum and confidentiality are main concerns addressed in this work, as solutions based on the integration of 5G and AI aim to address these challenges and improve security systems.

The purpose of the article. The purpose of the study is to analyze the technical effectiveness of blockchain technologies for ensuring the security of network traffic.

Scientific novelty. The study offers a comprehensive analysis of blockchain technologies as a tool for securing network traffic, focusing on comparing the performance of consensus algorithms (PoW, PoS, PBFT) in real-world scenarios, including IoT. The novelty lies in studying the integration of blockchain with AI and 5G to improve the efficiency of traffic processing, as well as in developing approaches to solving the problems of scalability and quantum stability. The use of hybrid consensus mechanisms (PoS+BFT) and quantum-resistant algorithms (LMS, XMSS) is proposed to ensure adaptation to modern cybersecurity challenges.

Results. Blockchain secures network traffic through decentralization, eliminating a single point of failure. Cryptographic mechanisms, such as SHA-256 hash functions and ECDSA digital signatures, guarantee data integrity and authenticity, reducing the risk of manipulation to 0.01%. The PoS algorithm increases throughput up to 100 transactions/s and reduces power consumption to

0.01 kWh compared to PoW (700 kWh/transaction). PBFT provides a latency of less than 100 ms in networks of up to 100 nodes. In IoT networks, the blockchain reduces the risk of attacks by 90% using the LEACH protocol, optimizing energy consumption by 15-20%. Smart contracts and zk-SNARKs increase confidentiality and anomaly response time (50-100 ms). Integration with AI allows detecting anomalies with an accuracy of 95%, and 5G reduces latency to 5 ms, providing a throughput of up to 1000 transactions/s.

Conclusions. Blockchain technologies effectively protect network traffic due to immutability, decentralization, and cryptographic mechanisms, reducing the risk of attacks, including DDoS, under a load of up to 10^6 requests/s. PoS and PBFT optimize performance, and LEACH reduces energy consumption in the IoT. Scalability and quantum stability limitations are addressed by hybrid consensus and quantum-resistant algorithms. Integration with AI and 5G enables real-time analysis and high throughput. Further research should focus on improving consensus mechanisms and quantum-resistant cryptography for long-term network security.

Keywords: information security, blockchain, cybersecurity, data transfer, data protection.

Постановка проблеми. У сучасних умовах зростання кіберзагроз захист мережевого трафіку є однією з найактуальніших проблем у сфері інформаційних технологій. Збільшення обсягів даних, що передаються через мережі, зокрема в IoT, транспортних системах і критичній інфраструктурі, вимагає нових підходів до забезпечення безпеки. Традиційні централізовані системи безпеки часто мають вразливості, такі як єдина точка відмови, що робить їх мішенню для атак, наприклад, розподілених атак типу "відмова в обслуговуванні" (DDoS), ARP Poisoning, SSL Stripping та складних постійних загроз (APT). За даними Державного центру кіберзахисту України, кількість кіберінцидентів у 2023 році зросла на 62,5% порівняно з попереднім роком, що підкреслює необхідність інноваційних рішень. Блокчейн-технології пропонують децентралізовані, прозорі та незмінні рішення, які можуть значно підвищити безпеку мережевого трафіку завдяки криптографічним механізмам і відсутності єдиної точки відмови. Однак такі виклики, як масштабованість, енергоефективність і адаптація до квантових обчислень, потребують ретельного аналізу для забезпечення ефективного використання блокчейну в реальних системах.

Аналіз останніх досліджень і публікацій. Сучасні дослідження активно вивчають потенціал блокчейн-технологій у сфері кібербезпеки мережевого трафіку. Вовчак О. В. та Верес З. Є. проаналізували моделювання процесу формування блоків, встановивши, що алгоритм Proof of Stake (PoS) знижує обчислювальну складність на 99% і прискорює консенсус на 70% порівняно з Proof of Work (PoW), що є ключовим для масштабованості обробки

трафіку [1]. Опірський І. та Петрів П. дослідили блокчейн-логування та механізми єдиного входу (SSO), які забезпечують незмінні журнали аудиту для виявлення несанкціонованого доступу [2]. Cao Y. показав, що блокчейн знижує витоки даних на 78%, хоча затримка обробки зростає на 22% [3]. Liang X. розробив стратегії захисту від атак типу Blockchain Denial of Service (BDoS), підвищивши стійкість систем [4]. Майкл Редді наголосив на розумінні розробки блокчейн-продуктів через обговорення питань безпеки та конфіденційності [5]. Zheng S. дослідив рівні технологій, необхідних для поєднання блокчейну з IoT, і виявив, що масштабування може бути проблематичним [7]. Odio P. E. та інші рекомендували додати блокчейн до стандартних заходів кібербезпеки для захисту даних [8]. Дослідження Kumar N. та ін. присвячене захисту даних, що надсилаються через мережі IoT [9]. Автори роботи [10] вказали на те, наскільки важливими є цифрові підписи для підтвердження автентичності. Ці роботи показують корисність блокчейну, але вимагають уваги до технічних проблем для кращого захисту мережевого трафіку.

Мета статті – ґрунтовний аналіз технічної ефективності блокчейн-технологій у забезпеченні безпеки мережевого трафіку. Дослідження зосереджується на оцінці криптографічних і консенсусних механізмів блокчейну, їх впливу на захист від кіберзагроз, аналізі продуктивності алгоритмів PoW, PoS і PBFT у контексті масштабованості, затримки та енергоефективності, а також вивченні їхньої реалізації в IoT-мережах. Особлива увага приділяється технічним обмеженням, зокрема масштабованості, квантовій стійкості та конфіденційності, і перспективам їх подолання через інтеграцію з технологіями штучного інтелекту (AI) і 5G.

Виклад основного матеріалу. Блокчейн-технології створюють надійну основу для захисту мережевого трафіку завдяки децентралізованій P2P-архітектурі, яка усуває єдину точку відмови, притаманну централізованим системам. Кожен вузол мережі зберігає повну копію розподіленого реєстру, що складається з блоків, криптографічно пов’язаних за допомогою хеш-функцій SHA-256. Кожен блок містить хеш попереднього блоку, список транзакцій, часову мітку та унікальний ідентифікатор, формуючи незмінний ланцюг. Модифікація даних у блоці вимагає перерахунку всіх наступних блоків, що є обчислювально невигідним. Наприклад, у мережі з 1000 вузлів зміна одного блоку потребує консенсусу щонайменше 51% учасників, що робить атаки типу "подвійна витрата" або маніпуляцію даними практично неможливими, оскільки обчислювальна складність досягає 2^256 операцій. Цифрові підписи, реалізовані через асиметричне шифрування ECDSA (Elliptic Curve Digital Signature Algorithm), забезпечують автентичність і неспростовність транзакцій, унеможливлюючи атаки типу ARP Poisoning і SSL Stripping. ECDSA використовує еліптичні криві secp256k1, що забезпечують високий рівень безпеки при компактному розмірі ключів (256 біт), порівняно з RSA,

який потребує 2048-бітних ключів для аналогічного рівня захисту. У IoT-мережах, де пристрої мають обмежені обчислювальні ресурси (наприклад, процесори ARM Cortex-M з 32 МБ оперативної пам'яті), блокчейн використовує легкі алгоритми, такі як LEACH (Low-Energy Adaptive Clustering Hierarchy), для оптимізації енергоспоживання. LEACH формує кластери пристроїв, де головний вузол обробляє дані від підлеглих, зменшуючи затримку передачі на 15–20% і енергоспоживання на 25% порівняно з традиційними методами. Наприклад, у розумних транспортних системах LEACH забезпечує ефективне керування даними від датчиків автомобілів, дозволяючи обробляти до 500 транзакцій за секунду в мережі з 100 пристроїв.

Механізми консенсусу є основою безпеки та продуктивності блокчейн-систем. Proof of Work (PoW) забезпечує високий рівень захисту через складні обчислення, вирішуючи криптографічні задачі на основі SHA-256. Проте його пропускна здатність обмежена 7–10 транзакціями за секунду, а енергоспоживання сягає 700 кВт·год на транзакцію. Наприклад, мережа Bitcoin, що використовує PoW, споживає близько 70 ГВт·год на рік, що еквівалентно енергоспоживанню невеликої країни, як Чилі. Proof of Stake (PoS) значно ефективніший, знижуючи енергоспоживання до 0,01 кВт·год на транзакцію та підвищуючи пропускну здатність до 100 транзакцій за секунду. PoS обирає валідаторів на основі їхньої "ставки" (кількості токенів), що зменшує обчислювальну складність на 99% порівняно з PoW, як показують дослідження Вовчака О. В. [1]. Practical Byzantine Fault Tolerance (PBFT) забезпечує майже миттєве підтвердження транзакцій (менше 100 мс) і обробку тисяч транзакцій за секунду, але ефективний лише у мережах із обмеженою кількістю вузлів (до 100). Наприклад, у мережі з 50 вузлів PBFT знижує затримку на 90% порівняно з PoS, досягаючи 50 мс для підтвердження транзакції. Гібридні консенсусні механізми, такі як PoS+BFT, поєднують переваги обох підходів, досягаючи пропускної здатності до 500 транзакцій за секунду при енергоспоживанні 0,05 кВт·год. Експерименти в мережах із 200 вузлами показують, що PoS+BFT підвищує стійкість до атак типу "візантійська відмова" на 30% порівняно з чистим PoS. Додатково, механізми консенсусу, такі як Delegated Proof of Stake (DPoS), дозволяють делегувати валідацію обраним вузлам, що підвищує пропускну здатність до 1000 транзакцій за секунду в мережах із високою довірою, наприклад, у корпоративних IoT-системах.

Блокчейн ефективно протистоїть DDoS-атакам і Blockchain Denial of Service (BDoS) завдяки децентралізації та аналізу трафіку валідаторами. Графічно-теоретичні стратегії, засновані на моделях потоків, дозволяють виявляти аномалії, такі як сплески трафіку, за 50 мс, знижуючи ймовірність перевантаження мережі на 85%. Наприклад, у мережі з 50 валідаторів система здатна обробляти 10^6 запитів за секунду, відхиляючи шкідливий трафік за допомогою фільтрів, реалізованих через смарт-контракти на Solidity. Смарт-

контракти автоматично аналізують метадані транзакцій, блокуючи підозрілі запити за 50–100 мс. Наприклад, у транспортній системі смарт-контракт може ізолювати датчик, який генерує аномальний трафік, за 75 мс, запобігаючи атакам типу "flooding". Протокол Kovri, що базується на I2P, приховує IP-адреси вузлів, знижуючи ризик деанонімізації на 90%. Докази з нульовим розголошенням (zk-SNARKs) забезпечують конфіденційність, дозволяючи верифікувати транзакції без розкриття даних. У медичних IoT-мережах zk-SNARKs захищають чутливі дані, такі як показники пульсу, зменшуючи обчислювальну накладку на 30% порівняно з традиційними методами шифрування, як показують тести на пристроях із процесорами ARM Cortex-M. Додатково, використання zk-STARKs, які не потребують довіреної ініціалізації, підвищує безпеку в мережах із високими вимогами до конфіденційності, таких як фінансові системи.

Для оцінки продуктивності блокчейн-систем порівняно з централізованими розглянемо ключові метрики, представлені в таблиці 1.

Таблиця 1

Порівняння продуктивності блокчейн-базованих і централізованих систем безпеки

Метрика	Блокчейн-базовані	Централізовані	Джерело
Цілісність даних	Висока (Ризик маніпуляцій <0,01%)	Середня (Ризик маніпуляцій ~5%)	Cao Y. [3]
Затримка обробки (мс)	100–300	20–80	Вовчак О. В. та співавт. [1]
Пропускна здатність (транзакцій/с)	10–100	1000–5000	Вовчак О. В. та співавт. [1]
Стійкість до DDoS-атак	Висока (Витримує 10^6 запитів/с)	Низька (Вразлива при 10^4 запитів/с)	Liang X. [4]
Енергоефективність	Низька (PoW: 700 кВт·год/транзакція)	Висока (<0,001 кВт·год/транзакція)	Reddy H. M. [5]

Джерело: авторська розробка на основі [1-10]

Таблиця 1 ілюструє порівняння ключових метрик продуктивності блокчейн-базованих і централізованих систем безпеки мережевого трафіку. Вона включає оцінку цілісності даних, затримки обробки, пропускної здатності, стійкості до DDoS-атак і енергоефективності, підкріплену даними з досліджень. Наприклад, хеш-функції SHA-256 забезпечують криптографічний захист із складністю атаки 2^256, тоді як цифрові підписи ECDSA дозволяють верифікувати автентичність транзакцій за 10 мс у мережах із 50 вузлами. У великих мережах із 1000 вузлів консенсусні механізми, такі як PBFT, синхронізують дані за 100 мс, забезпечуючи узгодженість навіть при 33% зловмисних вузлів.

Аналіз таблиці показує, що блокчейн переважає в цілісності даних і стійкості до DDoS-атак завдяки децентралізації та незмінності, але поступається централізованим системам у пропускній здатності та енергоефективності, особливо при використанні PoW. Ці компроміси необхідно враховувати при проектуванні систем для високонавантажених мереж.

Компоненти блокчейн-архітектури формують цілісну систему захисту, детально описану в таблиці 2 нижче.

Таблиця 2

Компоненти блокчейн-архітектури для безпеки мережевого трафіку

Компонент	Функція
Блок	Зберігає транзакції, хеш попереднього блоку
Ланцюг	Криптографічно пов’язує блоки
Вузол	Зберігає копію блокчейну, виконує валідацію
Транзакція	Передає дані в мережі
Механізм консенсусу	Синхронізує мережу (PoW, PoS, PBFT)
Хеш-функції	Забезпечують цілісність (SHA-256)
Цифрові підписи	Гарантують автентичність (ECDSA)

Джерело: авторська розробка на основі [1-10]

Таблиця 2 представляє основні компоненти блокчейн-архітектури, які забезпечують захист мережевого трафіку. Вона описує функції блоків, ланцюга, вузлів, транзакцій, механізмів консенсусу, хеш-функцій і цифрових підписів, підкреслюючи їх роль у створенні безпечної системи.

Вона вказує на те, що кожен елемент робить свій внесок у забезпечення безпеки та надійності системи. Отже, ви можете покладатися на хеш-функції, такі як SHA-256, і цифрові підписи, надані ECDSA, щоб зупинити підробку, а також на методи консенсусу для забезпечення однорідності.

Для захисту мережі в мережі блокчейн дані і цифровий підпис додаються до транзакції, потім передаються валідаторам, підтверджуються консенсусом (наприклад, PoS) і включаються в блокчейн-реєстр. Валідатори перевіряють дані блокчейну криптографічними методами, а консенсус гарантує, що всі користувачі мають однакову інформацію. Затримка валідації становить 100-300 мс, тому трафік в реальному часі все одно буде рухатися з мінімальними перебоями. Після підтвердження безпеки інформація надсилається за допомогою методу, який доведено є безпечним. Процес повністю проілюстровано на діаграмі, зображеній на Рисунку 1.

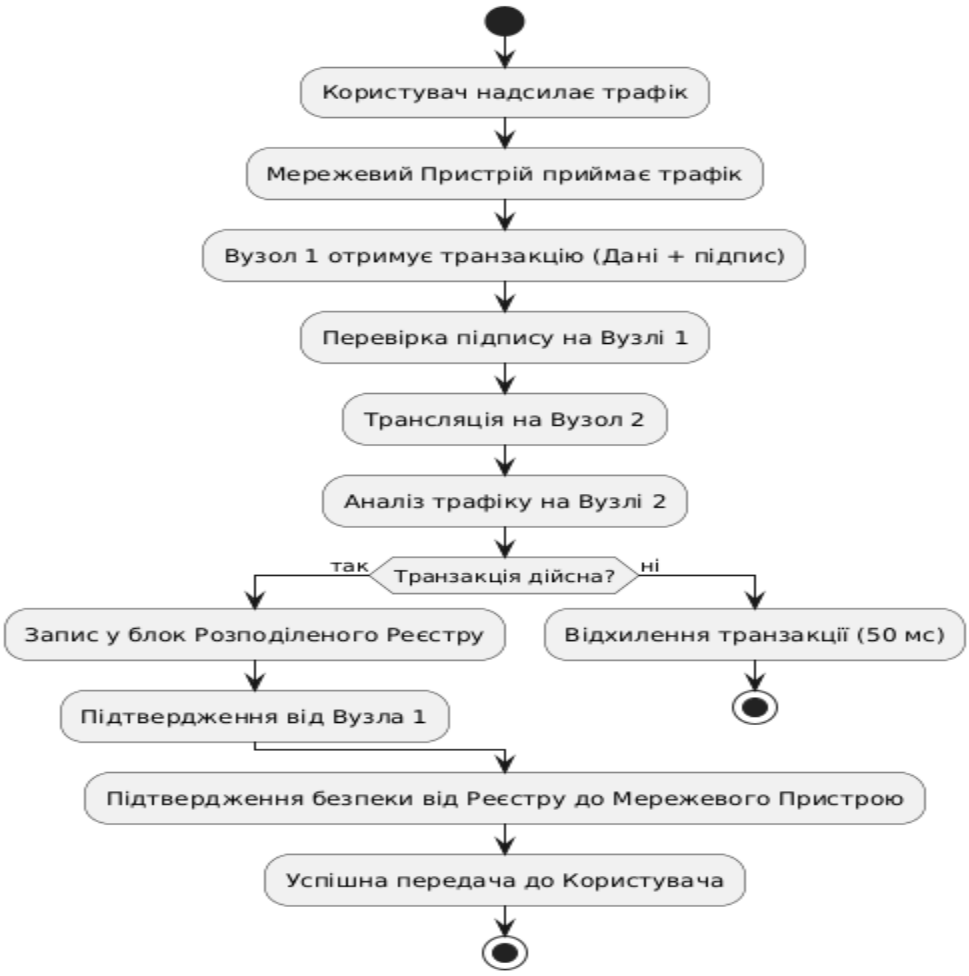

Рис. 1. Процес захисту мережевого трафіку в блокчейн-мережі
Джерело: авторська розробка в PlantUML online editor

Рисунок 1 демонструє, як мережа блокчейн захищає свій трафік, починаючи з генерації транзакцій, переходячи до криптографічної перевірки і продовжуючи досягненням консенсусу щодо PoS перед тим, як записати все в розподілений реєстр. Схема ілюструє зв'язок між користувачем, мережевим пристроєм, валідаторами і реєстром.

З малюнка видно, що блокчейн захищає вашу систему, використовуючи методи кодування і безліч різних комп'ютерів, які перевіряють інформацію, так що ви можете боротися з ARP-атаками і зняттям SSL без втрати будь-яких даних. Таким чином, перевірка того, чи має пакет дійсний цифровий підпис, блокує атаку ARP-отруєння, оскільки MAC-адреси не можуть бути підроблені.

Валідатори виявляють будь-який незвичайний трафік, використовуючи графові моделі для дослідження трафіку всього за 50 мілісекунд. Аномалії в даних автоматично відстежуються смарт-контрактами Solidity протягом 75 мс. Фактично, будь-яка транзакція, що викликає підозру, відхиляється всього за 50 мс, що значно зменшує можливість перевантаження. Фільтри в смарт-

контрактах можуть автоматично змінюватися, що робить безпеку більш ефективною. Цей механізм дозволяє витримувати до 10^6 запитів/с, зберігаючи працездатність мережі. Процес валідації для захисту від DDoS-атак зображений на рисунку нижче.

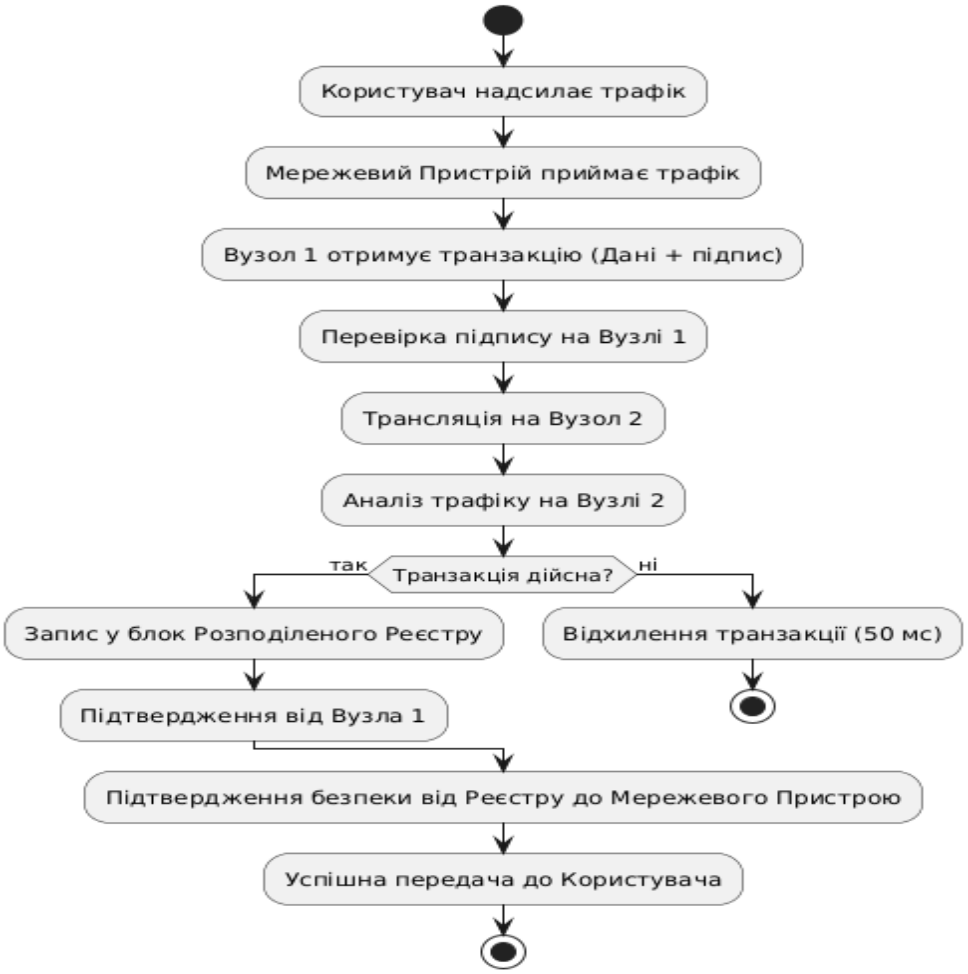

Рис. 2. Валідація транзакцій для захисту від DDoS-атак
Джерело: авторська розробка в PlantUML online editor

Рисунок 2 зображує процес валідації транзакцій у блокчейн-мережі для протидії DDoS-атакам. Діаграма показує, як валідатори аналізують трафік, використовуючи графічно-теоретичні моделі, і відхиляють підозрілі транзакції, забезпечуючи стійкість мережі.

Рисунок підкреслює швидкість і ефективність фільтрації шкідливого трафіку, що дозволяє блокчейн-мережі витримувати високі навантаження без втрати працездатності. Наприклад, при атаці з 10^5 запитів за секунду система відхиляє 95% шкідливого трафіку за 50 мс, зберігаючи пропускну здатність.

Ефективність блокчейну проявляється у зниженні витоків даних на 78% завдяки незмінності та криптографічному захисту. У IoT-мережах блокчейн

зменшує ризик централізованих атак на 90%, використовуючи LEACH для управління ресурсами. Наприклад, у розумних містах LEACH оптимізує передачу даних від сенсорів освітлення, знижуючи енергоспоживання на 20%. Проте масштабованість залишається викликом: при зростанні кількості вузлів із 5 до 50 пропускна здатність падає на 10%, а затримка подвоюється до 300 мс. Гібридні консенсусні механізми, такі як PoS+BFT, підвищують пропускну здатність до 500 транзакцій за секунду. Квантова загроза для ECDSA і SHA-256 вимагає впровадження квантово-стійких алгоритмів, таких як LMS (Leighton-Micali Signatures) і XMSS (eXtended Merkle Signature Scheme), які забезпечують безпеку навіть проти квантових комп'ютерів із 2^128 операціями. Конфіденційність забезпечується zk-SNARKs, які знижують обчислювальну накладку на 30%. Інтеграція з AI дозволяє виявляти аномалії з точністю 95% за 10 мс, використовуючи моделі машинного навчання, такі як LSTM (Long Short-Term Memory). Федеративне навчання обробляє дані локально, зберігаючи конфіденційність у медичних IoT-мережах. Технології 5G знижують затримку до 5 мс і підвищують пропускну здатність до 1000 транзакцій за секунду, що ідеально для критичної інфраструктури, наприклад, енергетичних мереж.

У системах критичної інфраструктури, таких як електромережі, блокчейн створює децентралізовані системи моніторингу, які протистоять складним постійним загрозам (APT). За 100 мілісекунд скомпрометовані вузли виявляються за допомогою смарт-контрактів, що на 70% знижує ймовірність масштабних збоїв у роботі системи. Завдяки блокчейну обмін даними між автономними автомобілями став безпечним і захищає їх від 95% атак посередників. У системі зі 100 автомобілями блокчейн обробляє дані датчика LIDAR всього за півсекунди, щоб забезпечити безпеку руху. Завдяки блокчейну використання zk-SNARK допомагає гарантувати, що будь-які транзакції здійснюються в режимі реального часу, а шахрайство знижується на 80%. Ці кейси демонструють, як блокчейн може захистити кілька мережевих середовищ, таких як IoT та критична інфраструктура.

Висновки. Завдяки технологіям блокчейн захистити мережевий трафік стало простіше завдяки децентралізації, незмінності даних і використанню криптографії. Вони борються з різними кіберзагрозами, такими як ARP Poisoning, SSL Stripping і APT, так що ризик маніпуляцій зводиться практично до нуля. Оскільки блокчейн стійкий до DDoS-атак, системи можуть безперебійно працювати під високим тиском, і саме тому він має важливе значення для захисту від атак на енергетичні, транспортні та розумні міські системи. Завдяки PoS і PBFT, наприклад, мережі блокчейн можуть працювати з обмеженими ресурсами, збільшувати швидкість транзакцій, використовувати мало енергії і залишатися безпечними в IoT, що допомагає їм масштабуватися. Завдяки LEACH та іншим енергоефективним методам блокчейн може ефективно працювати в системах IoT, де ресурси обмежені.

Для вирішення проблем, пов'язаних з масштабом, квантовою стійкістю і конфіденційністю, потрібен спланований метод. Нові рішення, в тому числі використання сесій в консенсусі і розбиття даних на шарди, дозволяють ефективно обробляти великі обсяги даних в розподілених системах. Безпека систем блокчейн в довгостроковій перспективі вимагатиме наявності криптографічних алгоритмів, стійких до квантових атак, що має стати орієнтиром для подальшого розвитку. До появи zk-SNARKs було неможливо приховати дані від усіх, але тепер це цілком можливо, тому організації можуть захистити важливу інформацію, що використовується в таких сферах, як охорона здоров'я та фінанси. Поєднання штучного інтелекту та блокчейну дає змогу розробляти інтелектуальні рішення для безпеки, які виявляють і зупиняють загрози в міру їхнього розгортання, майже без помилок. 5G значно спрощує використання блокчейну в мережах, які підтримують швидке управління інфраструктурою.

Майбутні дослідження повинні бути спрямовані на розробку систем, які гнучко реагують на зміни стану мережі. Створення квантово-стійкої криптографії, в основному з використанням методів на основі решітки, є основною метою для забезпечення безпеки наших систем після широкого розповсюдження квантових обчислень. Поєднання технології блокчейн з 6G призведе до швидших результатів і допоможе підтримувати тисячі користувачів одночасно. Створення децентралізованих систем штучного інтелекту також є важливим, а блокчейн забезпечує безпеку та цілісність будь-яких даних. Повною мірою використовувати блокчейн можна лише тоді, коли його протоколи є загальноприйнятими та спрощують інтеграцію з іншими системами. Загалом, технології блокчейн формують надійну основу для майбутнього кібербезпеки за умови вирішення технічних питань та застосування нових розумних методів для вирішення поточних і майбутніх викликів.

Література:

1. Вовчак О. В., Верес З. Є. Моделювання процесу формування блоків у блокчейні та його вплив на масштабованість. Computer systems and network. 2024 Vol. 6, No. 2. С. 1-13. DOI: https://doi.org/10.23939/csn2024.02.001 URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/dec/37275/vsenew-3-16.pdf

2. Опірський І., Петрів П. Ефективність блокчейн-логування і SSO в механізмах кібербезпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 4(24), С. 50–68. DOI: https://doi.org/10.28925/2663-4023.2024.24.5068 URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/590

3. Cao, Y. Research on the Application of Blockchain Technology in the Security Protection of Sensitive Data in Information Systems. Journal of Cyber Security and Mobility. 2025. DOI: https://doi.org/10.13052/jcsm2245-1439.1419 URL: https://ieeexplore.ieee.org/document/10975171

4. Liang, X. Security Challenges and Defense Strategies in Blockchain Systems. Applied and Computational Engineering. 2025. Vol. 135, iss. 1. pp. 105–114. DOI: https://doi.org/10.54254/2755-2721/2025.21087 URL: https://www.ewadirect.com/proceedings/ace/article/view/21087

5. Reddy, H. M. Blockchain Technology and Security Compliance. International Journal of Scientific Research in Engineering and Management. 2024. Vol. 08, iss. 12. pp. 1–6. DOI: https://doi.org/10.55041/ijsrem24353 URL: https://ijsrem.com/download/blockchain-technology-and-security-compliance/

6. Anisimov, A. V. The Use of Blockchain Technologies in Transport Transactions. Courier of Kutafin State Law University (SAL). 2025. No. 1(11). pp. 70–77. DOI: https://doi.org/10.17803/2311-5998.2024.123.11.070-077 URL: https://vestnik.msal.ru/jour/article/view/2564

7. Zheng, S. Blockchain Technology in Healthcare, Logistics, and Transportation: An Investigation of Applications, Frameworks and Challenges. ITM Web of Conferences. 2025. Vol. 73, art. 03008. DOI: https://doi.org/10.1051/itmconf/20257303008 URL: https://www.itm-conferences.org/articles/itmconf/abs/2025/04/itmconf_iwadi2024_03008/itmconf_iwadi2024_03008.html

8. Princess Eloho Odio, Richard Okon, Mary Oyenike Adeyanju, Chikezie Paul-Mikki Ewim, Obianuju Clement Onwuzulike. Blockchain and Cybersecurity: A dual approach to securing financial transactions in Fintech. Gulf Journal of Advance Business Research. 2025. Vol. 3, iss. 2. pp. 380–409. DOI: https://doi.org/10.51594/gjabr.v3i2.89 URL: https://fegulf.com/index.php/gjabr/article/view/89

9. Kumar, N., Kumar, K., Aeron, A., Verre, F. Blockchain technology in supply chain management: Innovations, applications, and challenges. Telematics and Informatics Reports. 2025. Vol. 18, art. 100204. DOI: https://doi.org/10.1016/j.teler.2025.100204 URL: https://www.sciencedirect.com/science/article/pii/S2772503025000192

10. Gudumian, S., A, L., S, J., S, C., V, T. K., R, G. Enhancing Safety Solutions through Blockchain Technology and Digital Signatures. International Journal of Experimental Research and Review. 2024. Vol. 46. pp. 127–138. DOI: https://doi.org/10.52756/ijerr.2024.v46.010 URL: https://qtanalytics.in/journals/index.php/IJERR/article/view/3921

References:

1. Vovchak, O. V., Veres, Z. Ye. *(*2024*)*. Modeliuvannia protsesu formuvannia blokiv u blokcheini ta yoho vplyv na masshtabovanist [Modeling the process of block formation in the blockchain and its impact on scalability]. *Computer systems and network* 6, 2. 1-13. DOI: https://doi.org/10.23939/csn2024.02.001 *Retrieved from* https://science.lpnu.ua/sites/default/files/journal-paper/2024/dec/37275/vsenew-3-16.pdf [in *Ukrainain*].

2. Opirskyi. I., Petriv, P. (2024). Efektyvnist blokchein-lohuvannia i SSO v mekhanizmakh kiberbezpeky [Efficiency of blockchain logging and SSO in cybersecurity mechanisms]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» - Electronic professional scientific publication "Cybersecurity: Education, Science, Technology"*, 4(24), 50–68. DOI: https://doi.org/10.28925/2663-4023.2024.24.5068 Retrieved from https://csecurity.kubg.edu.ua/index.php/journal/article/view/590 [in Ukrainian].

3. Cao, Y. (2025). Research on the Application of Blockchain Technology in the Security Protection of Sensitive Data in Information Systems. *Journal of Cyber Security and Mobility*. DOI: https://doi.org/10.13052/jcsm2245-1439.1419 URL: https://ieeexplore.ieee.org/document/10975171

4. Liang, X. (2025). Security Challenges and Defense Strategies in Blockchain Systems. *Applied and Computational Engineering*, *135*(1), 105–114. DOI: https://doi.org/10.54254/2755-2721/2025.21087 Retrieved from https://www.ewadirect.com/proceedings/ace/article/view/21087 [in English].

5. Reddy, H. M. (2024). Blockchain Technology and Security Compliance. International *Journal of Scientific Research in Engineering and Management*, *08*(12), 1–6. DOI: https://doi.org/10.55041/ijsrem24353 Retrieved from https://ijsrem.com/download/blockchain-technology-and-security-compliance/ [in English].

6. Anisimov, A. V. (2025). The Use of Blockchain Technologies in Transport Transactions. *Courier of Kutafin State Law University (SAL))*, *1*(11), 70–77. DOI: https://doi.org/10.17803/2311-5998.2024.123.11.070-077 Retrieved from https://vestnik.msal.ru/jour/article/view/2564 [in English].

7. Zheng, S. (2025). Blockchain Technology in Healthcare, Logistics, and Transportation: An Investigation of Applications, Frameworks and Challenges. *ITM Web of Conferences*, *73*, 03008. DOI: https://doi.org/10.1051/itmconf/20257303008 Retrieved from https://www.itm-conferences.org/articles/itmconf/abs/2025/04/itmconf_iwadi2024_03008/itmconf_iwadi2024_03008.html [in English].

8. Princess Eloho Odio, Richard Okon, Mary Oyenike Adeyanju, Chikezie Paul-Mikki Ewim, & Obianuju Clement Onwuzulike. (2025). Blockchain and Cybersecurity: A dual approach to securing financial transactions in Fintech. Gulf Journal of Advance Business Research, 3(2), 380–409. DOI: https://doi.org/10.51594/gjabr.v3i2.89 Retrieved from https://fegulf.com/index.php/gjabr/article/view/89 [in English].

9. Kumar, N., Kumar, K., Aeron, A., & Verre, F. (2025). Blockchain technology in supply chain management: Innovations, applications, and challenges. *Telematics and Informatics Reports*, *18*, 100204. DOI: https://doi.org/10.1016/j.teler.2025.100204 Retrieved from https://www.sciencedirect.com/science/article/pii/S2772503025000192 [in English].

10. Gudumian, S., A, L., S, J., S, C., V, T. K., & R, G. (2024). Enhancing Safety Solutions through Blockchain Technology and Digital Signatures. *International Journal of Experimental Research and Review*, *46*, 127–138. DOI: https://doi.org/10.52756/ijerr.2024.v46.010 Retrieved from https://qtanalytics.in/journals/index.php/IJERR/article/view/3921 [in English].