УДК 004.75 DOI 10.31673/2412-4338.2025.025697

Твердохліб Арсеній Олександрович
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0002-6591-2866

Лащевська Наталья Олександрівна
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID 0000-0003-2148-115X

МОДЕЛІ ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У ВИСОКОНАВАНТАЖЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ ДЛЯ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ТА ОБРОБКИ ДАНИХ

Анотація: *У статті здійснено комплексний аналіз застосування блокчейн-технологій у високонавантажених комп'ютерних системах для розподіленого зберігання та обробки даних. Особливу увагу приділено оцінці архітектурних підходів до інтеграції блокчейну в сучасні розподілені обчислювальні середовища, зокрема використанню смарт-контрактів, механізмів консенсусу та гібридних моделей зберігання інформації. Висвітлено основні переваги блокчейн-інфраструктури, такі як децентралізація, забезпечення цілісності даних, підвищена безпека та прозорість транзакцій.*

У рамках дослідження проведено детальний огляд сучасних рішень для розподіленого зберігання даних, що базуються на блокчейні, включаючи IPFS (InterPlanetary File System), Filecoin, Storj та їхню адаптацію до корпоративних і хмарних платформ. Особлива увага приділена питанням масштабованості блокчейн-мереж, продуктивності транзакцій та ефективності використання обчислювальних і енергетичних ресурсів, що є критично важливими аспектами для застосування блокчейну в високонавантажених системах.

Аналіз проведених досліджень дозволив виявити ключові переваги блокчейн-технологій у контексті розподіленого зберігання та обробки даних, зокрема їхню здатність до забезпечення стійкості до збоїв, відсутності єдиної точки відмови та захисту від несанкціонованого доступу. Водночас окреслено низку викликів, пов'язаних із високими витратами на енергоспоживання, необхідністю оптимізації алгоритмів консенсусу та розробкою ефективних підходів до управління великими масивами даних.

На основі отриманих результатів запропоновано концептуальні стратегії вдосконалення використання блокчейн-технологій у розподілених системах, зокрема через застосування комбінованих моделей обробки інформації, інтеграцію з хмарними обчисленнями та вдосконалення механізмів управління транзакціями. Представлені висновки можуть бути корисними для розробників блокчейн-рішень, науковців у сфері розподілених обчислень та фахівців з інформаційної безпеки.

Ключові слова**:** *блокчейн, розподілене зберігання, обробка даних, високонавантажені системи, безпека, масштабованість, смарт-контракти, консенсус, децентралізація.*

Tverdokhlib Arsenii
State university of information and communication technologies, Kyiv
ORCID 0000-0002-6591-2866

Lashchevska Nataliia
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0003-2148-115X

MODELS OF BLOCKCHAIN TECHNOLOGIES APPLICATION IN HIGH-LOAD COMPUTER SYSTEMS FOR DISTRIBUTED DATA STORAGE AND PROCESSING

Abstract: *This study presents a comprehensive analysis of the application of blockchain technologies in high-load computing systems for distributed data storage and processing. Particular attention is paid to evaluating architectural approaches for integrating blockchain into modern distributed computing environments, including the use of smart contracts, consensus mechanisms, and hybrid storage models. The study highlights the key advantages of blockchain infrastructure, such as decentralization, data integrity assurance, enhanced security, and transaction transparency.*

The research provides an in-depth review of contemporary blockchain-based distributed storage solutions, including IPFS (InterPlanetary File System), Filecoin, and Storj, along with their adaptation to corporate and cloud platforms. A special focus is placed on the challenges of blockchain scalability, transaction throughput, and efficient utilization of computational and energy resources, which are crucial for its implementation in high-load systems. Additionally, the study explores the impact of blockchain adoption on overall system performance and potential trade-offs between security, efficiency, and resource consumption.

Through an extensive review of existing research and practical implementations, the study identifies the core benefits of blockchain for distributed storage and processing. These include resilience to system failures, elimination of single points of failure, and protection against unauthorized data access. At the same time, several critical challenges are outlined, such as high energy consumption, the need for optimizing consensus algorithms, and developing effective strategies for managing large-scale data volumes. The research also investigates the economic implications of blockchain deployment, assessing cost-effectiveness in different operational contexts.

Based on the findings, the study proposes conceptual strategies for optimizing blockchain utilization in distributed computing systems. These strategies include the implementation of hybrid data processing models, integration with cloud computing, and enhancements in transaction management mechanisms. The insights provided in this study may be valuable for blockchain solution developers, researchers in distributed computing, and cybersecurity professionals, offering a robust foundation for further advancements in the field.

Keywords: *blockchain, distributed storage, data processing, high-load systems, security, scalability, smart contracts, consensus, decentralization.*

1.Вступ

У сучасних інформаційних технологіях зростаючий обсяг цифрових даних, що генерується підприємствами, урядовими структурами та користувачами, вимагає надійних, масштабованих і безпечних рішень для зберігання та обробки. Традиційні централізовані моделі, такі як серверні кластери та хмарні платформи, забезпечують високу продуктивність і доступність, проте мають обмеження щодо безпеки, централізації управління та ризику несанкціонованого доступу.

Блокчейн є інноваційною технологією, що забезпечує децентралізоване, розподілене та незмінне зберігання даних, підвищуючи їхню безпеку та стійкість до збоїв. Спочатку відомий як основа криптовалют, зокрема Bitcoin та Ethereum, блокчейн сьогодні розглядається як перспективне рішення для фінансів, логістики, охорони здоров’я, енергетики та управління

персональними даними. Його застосування у високонавантажених комп'ютерних системах відкриває нові можливості, серед яких усунення централізованих точок відмови, підвищення безпеки через криптографічний захист і механізми консенсусу, забезпечення прозорості та незмінності записів, а також автоматизація обробки даних за допомогою смарт-контрактів. Однак масштабованість блокчейн-систем залишається викликом.

Традиційні алгоритми консенсусу, такі як Proof-of-Work та Proof-of-Stake, мають обмежену продуктивність, що ускладнює обробку великих обсягів даних у реальному часі. Високе енергоспоживання PoW-мереж також обмежує їхнє використання у сценаріях, що потребують швидкості та мінімальних витрат ресурсів.

У цій статті проаналізовано сучасні підходи до інтеграції блокчейну в розподілені системи зберігання та обробки даних, зокрема децентралізовані файлові системи, такі як IPFS, Storj та Filecoin. Оцінено їхню сумісність із блокчейн-архітектурами та розглянуто виклики, пов'язані з продуктивністю, масштабованістю та енергоефективністю. Крім того, запропоновано концептуальні підходи до оптимізації блокчейн-технологій, що сприятимуть побудові безпечних, надійних і продуктивних систем, придатних для критично важливих галузей.

2. Аналіз літературних даних і постановка проблеми

Розподілене зберігання та обробка даних є критично важливими компонентами сучасних високонавантажених комп'ютерних систем. У зв'язку з експоненційним зростанням обсягів інформації традиційні централізовані рішення, такі як класичні бази даних, серверні сховища та хмарні платформи, забезпечують високу продуктивність і доступність. Водночас вони мають низку недоліків, зокрема централізовані точки відмови, вразливість до кібератак, залежність від постачальників послуг та значні витрати на безпеку. У цьому контексті блокчейн-технологія пропонує принципово інший підхід до зберігання та обробки інформації, заснований на децентралізації, криптографічному захисті та незмінності записів. Завдяки цим властивостям блокчейн здатен забезпечити підвищену безпеку, надійність та стійкість до збоїв, що підтверджується численними науковими дослідженнями.

Аналіз наукової літератури свідчить про значний інтерес до інтеграції блокчейну у сферу управління даними, що проявляється у дослідженнях щодо його безпеки, продуктивності та масштабованості. Зокрема, у працях [1, 2] доведено, що блокчейн мінімізує ризики компрометації даних і несанкціонованого доступу через використання криптографічного шифрування та механізмів консенсусу. Водночас у дослідженнях [3, 4] акцентується увага на проблемах масштабованості та продуктивності, які обмежують ефективність блокчейн-мереж при роботі з великими обсягами інформації. Одним із перспективних напрямів є поєднання блокчейн-інфраструктури з іншими технологіями, такими як хмарні обчислення, розподілені файлові системи (наприклад, IPFS, Storj, Filecoin) та механізми масштабованого консенсусу, що дозволяють зменшити навантаження на блокчейн-мережу [5]. Важливим є також удосконалення алгоритмів консенсусу, зокрема Proof-of-Stake (PoS) та його модифікацій (Delegated PoS, Proof-of-Authority тощо), які демонструють покращену продуктивність і знижене енергоспоживання порівняно з традиційним Proof-of-Work (PoW).

Останні дослідження показують, що ефективне використання блокчейну у високонавантажених системах можливе через багаторівневі архітектури, що поєднують централізовані та децентралізовані підходи до управління даними [6]. Наприклад, у роботах [7, 8] розглядаються гібридні моделі, де критично важливі дані зберігаються у блокчейні, а менш значущі – у децентралізованих файлових системах. Водночас залишаються відкритими ключові питання, що потребують подальших досліджень: оптимізація масштабованості блокчейн-систем для високонавантажених середовищ, удосконалення механізмів консенсусу для ефективної обробки транзакцій, забезпечення балансу між безпекою та швидкістю доступу до інформації, а

також розробка енергоефективних рішень, що знижують витрати на підтримку блокчейн-інфраструктури.

Отже, попри значний потенціал блокчейн-технологій у сфері розподіленого зберігання та обробки даних, їхня інтеграція у високонавантажені комп'ютерні системи потребує подальших досліджень для створення ефективних, безпечних і масштабованих рішень.

3. Мета і задачі дослідження

Метою даного дослідження є комплексний аналіз можливостей застосування технології блокчейн у сфері розподіленого зберігання та обробки даних у високонавантажених комп'ютерних системах. Крім того, дослідження спрямоване на розробку концептуальних підходів, що сприятимуть підвищенню ефективності, масштабованості та безпеки таких систем. Важливість цієї тематики зумовлена зростаючими вимогами до збереження великих обсягів інформації, необхідністю забезпечення їхньої безпеки та потребою в оптимізації розподілених обчислювальних ресурсів.

Для досягнення поставленої мети передбачається вирішення низки ключових завдань. Передусім необхідно здійснити аналіз сучасних методів розподіленого зберігання та обробки даних, що включає огляд існуючих централізованих і децентралізованих рішень, оцінку їхніх переваг і недоліків з позиції продуктивності, надійності та безпеки. Важливим аспектом дослідження є вивчення можливостей інтеграції блокчейн-технологій у розподілені обчислювальні середовища, що передбачає аналіз різних блокчейн-архітектур, механізмів консенсусу та підходів до збереження великих обсягів інформації. Зокрема, розглядаються алгоритми PoW, PoS, Delegated PoSта їхній вплив на швидкість обробки транзакцій і загальну ефективність роботи високонавантажених систем.

Одним із центральних аспектів дослідження є оцінка продуктивності та масштабованості блокчейн-систем, що включає аналіз впливу вибору алгоритмів консенсусу на пропускну здатність мережі та ефективність зберігання даних. Водночас розробка концептуальної моделі використання блокчейну для розподіленого зберігання має на меті створення підходу, що дозволяє оптимізувати використання ресурсів, знизити навантаження на блокчейн-мережу та підвищити рівень безпеки збереженої інформації. Особливу увагу приділено оцінці можливих ризиків та обмежень блокчейн-технологій, що передбачає виявлення основних загроз, таких як ризики компрометації даних, вразливість до атак та високе енергоспоживання, а також аналіз шляхів їхньої мінімізації.

У межах дослідження розглядаються перспективи застосування блокчейну в умовах високонавантажених комп'ютерних систем, визначаються галузі, у яких децентралізовані технології можуть продемонструвати найбільшу ефективність, а також оцінюється економічна доцільність їхнього впровадження.

4.1 Архітектурні підходи до використання блокчейну у розподілених системах

Технологія блокчейн відкриває нові перспективи для організації розподілених систем зберігання та обробки даних, забезпечуючи децентралізацію, безпеку й прозорість. У сучасних високонавантажених системах актуальною залишається проблема збереження значних обсягів інформації з гарантією її цілісності та доступності. Традиційні централізовані підходи, такі як класичні бази даних і хмарні платформи, демонструють високу продуктивність, проте супроводжуються загрозами атак, централізованими точками відмови та суттєвими витратами на безпеку. У цьому контексті застосування децентралізованих файлових систем, таких як IPFS, Filecoin та Storj, сприяє підвищенню надійності завдяки унікальній системі адресації контенту та розподіленій інфраструктурі.

Важливим напрямом розвитку є поєднання блокчейну з хмарними обчисленнями, що дозволяє оптимізувати використання обчислювальних ресурсів. Гібридні моделі передбачають використання блокчейну для контролю доступу та автентифікації даних, тоді як основні інформаційні масиви зберігаються у хмарних дата-центрах, поєднуючи безпеку децентралізації з ефективністю централізованих платформ. Крім того, блокчейн сприяє автоматизації управління доступом до інформації шляхом впровадження смарт-контрактів, що дозволяють забезпечувати безперебійну перевірку прав доступу та фіксацію змін у системі без залучення посередників. Це особливо важливо у фінансових та правових аспектах, де смарт-контракти забезпечують надійне виконання умовних операцій.

Інтеграція блокчейну в розподілені обчислювальні середовища, як-от Golem або iExec, дозволяє створювати інфраструктуру децентралізованих обчислень, де вузли мережі виконують завдання без потреби централізованого контролю. Такий підхід сприяє масштабованості та ефективному розподілу навантаження між учасниками. Водночас удосконалення механізмів консенсусу є ключовим фактором підвищення продуктивності блокчейн-систем. Використання шардінгу, сайдчейнів та рішень Layer 2, зокрема Lightning Network і Plasma, дає змогу суттєво покращити пропускну здатність, зменшити затримки та підвищити ефективність обробки транзакцій.

Таблиця 1

Порівняння децентралізованих файлових систем

Характеристика	IPFS	Filecoin	Storj
Тип зберігання	Децентралізоване розподілене сховище	Децентралізоване зберігання з економічними стимулами	Децентралізоване хмарне сховище
Механізм консенсусу	Відсутній (однорангова мережа)	Proof-of-Replication, Proof-of-Spacetime	Відсутній, розподілена інфраструктура
Безпека даних	Хешування файлів, перевірка цілісності	Шифрування, підтвердження збереження	Шифрування файлів, поділ на фрагменти
Модель оплати	Безкоштовне використання	Плата за використання зберігання	Передплата або плата за використання
Продуктивність	Висока (залежить від вузлів)	Середня (залежить від вузлів і тарифів)	Висока (оптимізовано для швидкого доступу)
Основне використання	Обмін файлами, розподілене сховище	Комерційне зберігання, дата-центри	Хмарне зберігання, корпоративні рішення

Застосування блокчейну у критично важливих сферах, таких як фінанси, медицина та державне управління, відкриває нові можливості для підвищення рівня безпеки та прозорості. У фінансовій сфері блокчейн мінімізує ризики маніпуляцій з історією платежів, у медичній галузі забезпечує захист електронних записів пацієнтів, а у державному управлінні сприяє ефективному захисту персональних даних і прозорості адміністративних процесів. Незважаючи на значний потенціал, масштабне впровадження блокчейн-рішень потребує подальшого вдосконалення у

сфері продуктивності, зберігання великих обсягів даних і регуляторної інтеграції. Розвиток нових підходів до управління даними та оптимізація алгоритмів консенсусу сприятимуть подальшому зміцненню позицій блокчейну у високонавантажених комп'ютерних системах.

4.2 Проблеми продуктивності та масштабованості

Попри значний потенціал блокчейну у сфері безпеки та децентралізації, його застосування у високонавантажених системах стикається з проблемами продуктивності та масштабованості. Базові блокчейн-архітектури, зокрема Bitcoin та Ethereum, обмежені через складність механізмів консенсусу, необхідність підтвердження кожної транзакції більшістю вузлів та зростання розміру реєстру. Порівняно з централізованими системами, такими як Visa, які можуть обробляти понад 24 000 транзакцій за секунду, традиційні блокчейн-рішення демонструють значно нижчу ефективність: Bitcoin обробляє близько 7 транзакцій за секунду, а Ethereum – приблизно 30, що значно обмежує його використання у масштабних бізнес-застосуваннях.

Основною причиною низької продуктивності є механізм консенсусу. Алгоритм PoW, що застосовується у Bitcoin та Ethereum 1.0, вимагає значних обчислювальних ресурсів, а процес майнінгу ускладнює використання технології у середовищах із високим навантаженням. Перехід на PoS у Ethereum 2.0 дозволяє значно підвищити продуктивність, зменшивши енергоспоживання, що сприяє обробці понад 100 000 транзакцій за секунду. Подібні механізми використовуються в Algorand та Hedera Hashgraph, забезпечуючи швидку та ефективну перевірку операцій.

Сучасні методи масштабування блокчейну передбачають використання шардінгу, який розподіляє мережу на незалежні частини, що паралельно обробляють транзакції. Цей підхід застосовується у Polkadot, Ethereum 2.0 та Near Protocol, забезпечуючи суттєве зростання пропускної здатності. Сайдчейни, такі як RSK (Rootstock), дозволяють зменшити навантаження на основний ланцюг, виконуючи транзакції у паралельних блокчейнах. Альтернативою є рішення рівня Layer 2, зокрема Lightning Network для Bitcoin та Rollups для Ethereum, які здійснюють транзакції поза основною мережею, підтверджуючи їх у блокчейні лише після завершення. Додатково інтеграція з децентралізованими файловими системами, такими як IPFS та Filecoin, оптимізує зберігання даних, залишаючи у блокчейні лише хеші файлів.

Обмежена швидкість транзакцій та висока енергетична вартість ускладнюють використання блокчейну у критичних системах. У фінансовому секторі низька продуктивність обмежує конкуренцію з традиційними платіжними платформами, тоді як у медицині блокчейн-реєстри вимагають високої швидкості обробки для ефективного збереження медичних даних. У логістиці технологія забезпечує безпечне відстеження постачань, знижуючи ризики шахрайства. Водночас високий рівень енергоспоживання, зокрема у Bitcoin, робить традиційні блокчейни менш ефективними з погляду сталого розвитку. Перехід до PoS та подальші дослідження у сфері оптимізації споживання енергії є необхідними для адаптації блокчейну до реальних застосувань.

Отже, продуктивність та масштабованість є ключовими викликами для впровадження блокчейну у високонавантажених системах. Традиційні алгоритми консенсусу мають значні обмеження, що ускладнює їхнє використання у реальному часі. Застосування PoS, шардінгу, сайдчейнів та рішень рівня Layer 2 сприяє підвищенню ефективності блокчейн-мереж. Подальші дослідження у цьому напрямі сприятимуть розвитку високопродуктивних децентралізованих архітектур, здатних конкурувати із централізованими системами у сфері зберігання та обробки даних.

Таблиця 2

Порівняння продуктивності блокчейн-мереж

Блокчейн-система	Алгоритм консенсусу	Продуктивність (транзакцій/сек)	Енергоспоживання (МВт/год на транзакцію)
Bitcoin	Proof-of-Work	7	707
Ethereum	Proof-of-Work	30	83
Ethereum 2.0	Proof-of-Stake	100000	0.0026
Polkadot	Nominated PoS	1000	0.02
Solana	Proof-of-History	65000	0.002

4.3 Безпека та надійність розподіленого зберігання на основі блокчейну

Блокчейн-технологія забезпечує високий рівень безпеки даних завдяки своїй децентралізованій структурі, криптографічним механізмам захисту та незмінності записів. Однак, попри ці переваги, вона не є абсолютно захищеною і може піддаватися різним видам атак, включаючи компрометацію механізмів консенсусу, вразливості смарт-контрактів, загрози централізації вузлів і проблеми управління доступом.

Захист даних у блокчейні ґрунтується на криптографічних методах, що забезпечують незмінність транзакцій, унеможливлюючи їхню модифікацію без зміни всієї структури реєстру. Такий підхід особливо цінний у фінансових та державних системах, але створює виклики щодо відповідності нормативним вимогам, зокрема у контексті "права на забуття" згідно з GDPR.

Серед основних загроз слід виокремити атаку 51%, яка виникає за умови контролю зловмисником понад 50% потужностей мережі, що дозволяє змінювати історію транзакцій. Така небезпека особливо актуальна для малих блокчейнів із низькою кількістю активних вузлів. Використання алгоритмів консенсусу на кшталт PoS, де валідатори повинні мати значні фінансові вкладення, знижує ймовірність такої атаки. Іншою серйозною загрозою є атака Sybil, яка передбачає створення великої кількості фальшивих вузлів для отримання контролю над процесом перевірки блоків. Захист від неї забезпечується застосуванням механізмів консенсусу, що потребують економічних витрат, таких як PoW, PoS або Proof-of-Authority.

Управління доступом у блокчейні має принципово інший підхід порівняно з централізованими системами, де контроль здійснюється адміністраторами. Смарт-контракти дозволяють автоматизувати контроль доступу, що є ключовим аспектом у децентралізованих системах зберігання, таких як IPFS чи Storj. Крім того, оскільки більшість публічних блокчейнів є відкритими, існує ризик витоку конфіденційної інформації. Для його мінімізації використовуються технології анонімних транзакцій, такі як zk-SNARKs, що дозволяють підтверджувати операції без розкриття їхнього змісту, вже інтегровані у Monero та Zcash.

Додаткову загрозу становлять атаки на смарт-контракти, що можуть призводити до втрати активів через помилки у коді. Відомий випадок – експлойт The DAO у 2016 році, що спричинив втрату понад 60 мільйонів доларів. Для підвищення безпеки застосовуються аудит коду, формальна верифікація та автоматизовані засоби аналізу, такі як MythX чи Slither.

Фізична безпека вузлів мережі також є важливим фактором, оскільки втрата значної кількості нод, наприклад, унаслідок кібератак або природних катастроф, може порушити функціонування блокчейну. Реплікація даних між вузлами мінімізує подібні ризики, зберігаючи цілісність системи навіть у разі значних збоїв.

Регуляторні вимоги додають ще один рівень складності у сфері блокчейн-безпеки. Оскільки реєстр блокчейну є незмінним, це суперечить принципам, таким як "право на видалення даних".

Одним із рішень є гібридні моделі зберігання, де чутливі дані шифруються та зберігаються поза блокчейном, а в реєстрі містяться лише хеші для підтвердження автентичності інформації.

Таким чином, безпека блокчейну є багаторівневим завданням, що включає криптографічний захист, механізми консенсусу, управління доступом, аудит смарт-контрактів та відповідність регуляторним вимогам. Подальші дослідження у сферах постквантової криптографії та анонімних транзакцій можуть сприяти підвищенню стійкості технології до потенційних атак, що зробить її ще більш надійною у довгостроковій перспективі.

4.4 Перспективи та напрямки розвитку блокчейн-технологій у розподіленому зберіганні та обробці даних

У сучасних умовах технологія блокчейн продовжує динамічно розвиватися, відкриваючи нові перспективи у сфері децентралізованого зберігання та обробки даних. Постійне зростання обсягів інформації, зростаючі вимоги до безпеки та необхідність усунення централізованих посередників стимулюють розробку інноваційних рішень, спрямованих на підвищення продуктивності, масштабованості та ефективності управління ресурсами. Одним із ключових напрямків є інтеграція блокчейну з технологіями штучного інтелекту, що сприяє створенню надійних механізмів збереження та обробки навчальних даних, мінімізуючи ризики маніпуляцій і підробок. Крім того, застосування смарт-контрактів дозволяє автоматизувати верифікацію інформації, що є критично важливим для забезпечення прозорості децентралізованих нейромереж.

Сучасні дослідження також свідчать про значний потенціал гібридних блокчейн-архітектур, які поєднують переваги приватних і публічних реєстрів, забезпечуючи високу продуктивність та безпеку. Наприклад, приватний блокчейн може використовуватися для оперативної обробки транзакцій, а публічний – для їхньої незалежної перевірки та довготривалого збереження. Це особливо важливо у фінансовому секторі, де гарантування конфіденційності даних є ключовим аспектом. Водночас технологія набуває популярності в державному управлінні, зокрема для реєстрації прав власності, ведення офіційних реєстрів та електронного голосування.

Окремої уваги заслуговує проблема енергоефективності блокчейн-мереж, що залишається актуальним викликом для їхнього масового впровадження. Традиційні механізми консенсусу, зокрема PoW, супроводжуються значними енергетичними витратами, що робить їх екологічно неефективними. Альтернативні підходи, такі як PoS, Proof-of-Authority та Proof-of-Space-Time, дозволяють суттєво знизити споживання електроенергії, забезпечуючи більш сталий розвиток блокчейн-індустрії. Показовим у цьому контексті є перехід мережі Ethereum на PoS, що відкриває шлях до широкомасштабного впровадження екологічно чистих технологій.

Подальший розвиток блокчейну нерозривно пов’язаний із технологіями шарового масштабування, які дозволяють суттєво підвищити швидкість обробки транзакцій без перевантаження основної мережі. Рішення рівня Layer 2, такі як Lightning Network та zk-Rollups, вже демонструють високу ефективність, особливо у сфері розподіленого зберігання даних. Децентралізовані хмарні платформи, зокрема Filecoin, Storj та Sia, пропонують альтернативу традиційним централізованим сховищам, дозволяючи користувачам безпечно обмінюватися інформацією без посередників. Подальші дослідження у цій галузі спрямовані на покращення швидкості доступу до даних та інтеграцію з сучасними обчислювальними технологіями, такими як edge computing.

Перспективним напрямом розвитку є також застосування блокчейну в Інтернеті речей (IoT). Використання розподілених реєстрів дає змогу пристроям безпечно обмінюватися даними без залучення централізованих серверів, що суттєво підвищує рівень безпеки IoT-інфраструктури. Це зменшує ризики кібератак, оптимізує навантаження на центри обробки даних та підвищує

автономність пристроїв. Поряд із цим, розвиток постквантової криптографії стає критично важливим для забезпечення довготривалої безпеки блокчейн-систем. З огляду на можливу появу квантових комп'ютерів, традиційні криптографічні алгоритми можуть стати вразливими, тому вже сьогодні ведуться активні дослідження з впровадження стійких до квантових обчислень методів шифрування.

Зважаючи на всі зазначені аспекти, можна зробити висновок, що блокчейн-технології продовжать активно розвиватися, змінюючи підходи до зберігання, обробки та управління даними. Масове впровадження блокчейну у сферу високонавантажених обчислень стане можливим за умови подальшої оптимізації масштабованих, безпечних та енергоефективних рішень. Враховуючи сучасні тенденції, технологія блокчейн має всі передумови для перетворення на один із ключових елементів цифрової економіки майбутнього.

5. Аналіз результатів дослідження

Проведене дослідження дозволило оцінити ефективність застосування блокчейн-технологій для розподіленого зберігання та обробки даних, а також виявити ключові переваги й обмеження цієї технології. Аналіз сучасних блокчейн-архітектур засвідчив, що вони забезпечують високий рівень безпеки завдяки використанню криптографічного шифрування, децентралізації та механізмів консенсусу. Основною перевагою блокчейну є його здатність створювати незмінні реєстри, що виключає можливість фальсифікації даних та мінімізує ризик атак. Водночас ідентифіковано низку технічних і концептуальних обмежень, які ускладнюють його широкомасштабне впровадження у високонавантажені комп'ютерні системи.

Дослідження продуктивності блокчейн-мереж підтвердило, що традиційні механізми консенсусу, зокрема PoW, характеризуються низькою пропускною здатністю, що значно поступається централізованим системам. Зокрема, блокчейни на основі PoW, такі як Bitcoin, обробляють лише кілька транзакцій за секунду, тоді як централізовані фінансові платформи, такі як Visa, мають пропускну здатність у десятки тисяч операцій. Це створює суттєві обмеження для використання блокчейну в сценаріях, що потребують високої швидкодії. Однак сучасні механізми консенсусу, такі як PoS та Delegated PoS, демонструють значно кращу продуктивність та енергоефективність, що робить їх перспективними для розподілених сховищ та обчислювальних середовищ.

Аналіз методів масштабування блокчейн-систем вказує на те, що технології другого рівня, такі як Layer 2-рішення, шардінг та сайдчейни, відіграють ключову роль у підвищенні ефективності. Зокрема, zk-Rollups дозволяють групувати велику кількість транзакцій поза основним блокчейном, що зменшує навантаження на мережу та підвищує швидкість обробки даних. Такий підхід дозволяє зберігати високу продуктивність систем, забезпечуючи при цьому безпеку та достовірність записів.

Дослідження питань безпеки блокчейн-мереж виявило низку загроз, серед яких атаки 51%, атаки Sybil, вразливості смарт-контрактів та ризики витоку конфіденційної інформації. Використання PoS значно зменшує ймовірність атак 51%, оскільки для отримання контролю над мережею зловмиснику необхідно володіти значними ресурсами. Додатково застосування механізмів Zero-Knowledge Proof, зокрема zk-SNARKs, дозволяє забезпечити конфіденційність транзакцій та зменшити ймовірність витоку персональних даних.

Аналіз перспектив інтеграції блокчейну з децентралізованими файловими системами, такими як IPFS, Filecoin та Storj, засвідчив, що такі гібридні рішення сприяють оптимізації ресурсів мережі. Зокрема, ці підходи дають змогу використовувати блокчейн лише для перевірки достовірності даних, а самі файли зберігати у зовнішніх розподілених сховищах, що забезпечує баланс між продуктивністю та безпекою, водночас зменшуючи витрати на обробку інформації.

Результати дослідження також підтверджують високий потенціал блокчейн-технологій у сфері державного управління, охорони здоров'я, фінансових технологій та Інтернету речей (IoT). Наприклад, у державному секторі блокчейн може бути використаний для управління реєстрами та організації виборчих процесів, що сприятиме зниженню рівня корупційних ризиків. У фінансовій сфері децентралізовані реєстри забезпечують підвищену прозорість операцій, що сприяє довірі між учасниками ринку. У контексті Інтернету речей блокчейн може слугувати засобом для безпечної взаємодії між пристроями, запобігаючи несанкціонованому доступу та маніпуляціям з даними.

Отже, блокчейн є перспективною технологією для розподіленого зберігання та обробки даних, однак його ефективна імплементація потребує подальшого вдосконалення механізмів консенсусу, розробки нових моделей масштабування та покращення методів забезпечення конфіденційності транзакцій.

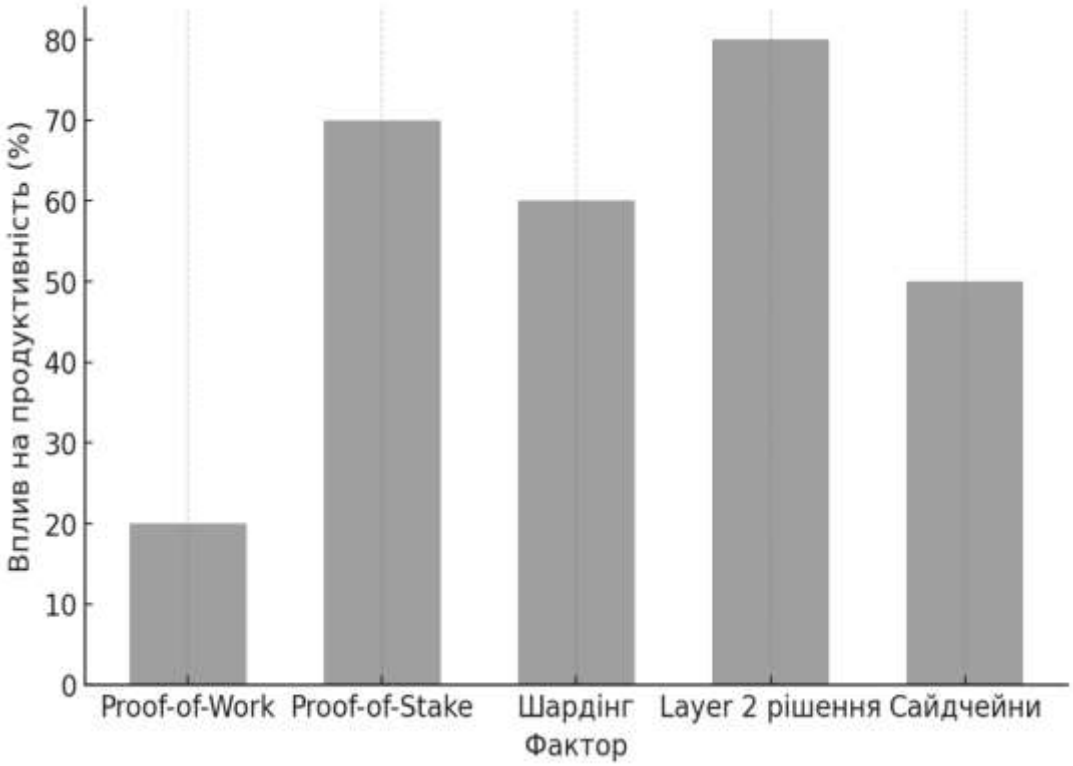

Рис. 1. Вплив різних факторів на продуктивність блокчейн-систем

6. Висновки

Дане дослідження дозволило оцінити потенціал блокчейн-технологій у контексті розподіленого зберігання та обробки даних, виявивши їхні ключові переваги та обмеження. Встановлено, що завдяки децентралізації, незмінності даних та криптографічному захисту блокчейн забезпечує високий рівень довіри серед учасників мережі, усуваючи необхідність у централізованих посередниках. Водночас аналіз існуючих підходів засвідчив, що централізовані системи зберігають домінуючі позиції завдяки вищій продуктивності, незважаючи на їхню вразливість до атак та ризик централізованих точок відмови. Натомість блокчейн, усуваючи ці недоліки, стикається з проблемами масштабованості та енергоефективності.

Дослідження продуктивності блокчейн-систем підтвердило, що традиційні алгоритми консенсусу, зокрема PoW, обмежують пропускну здатність мережі та вимагають значних

енергетичних витрат. Зокрема, Bitcoin здатний обробляти лише сім транзакцій за секунду, тоді як централізовані фінансові системи демонструють у тисячі разів вищу швидкість. Водночас альтернативні механізми, такі як PoS і Delegated PoS, суттєво підвищують продуктивність, одночасно зменшуючи енергоспоживання, що робить їх перспективними для високонавантажених розподілених систем.

Аналіз масштабованості блокчейну вказує на необхідність впровадження додаткових технологій, таких як Layer 2-рішення, шардінг та сайдчейни. Зокрема, zk-Rollups сприяють зменшенню навантаження на основну мережу, агрегуючи транзакції перед їхнім записом у блокчейн. Такі підходи підвищують ефективність мережі, дозволяючи її інтеграцію в критично важливі сфери, як-от фінансові операції та керування цифровими активами.

Безпекові аспекти блокчейн-систем залишаються одним із ключових викликів для широкого впровадження технології. Дослідження засвідчило, що хоча блокчейн ефективно протидіє підробці даних, він не позбавлений загроз. Зокрема, атака 51% залишається ризиком для мереж із низькою капіталізацією, а атака Sybil та вразливості смарт-контрактів створюють додаткові загрози. Використання механізмів PoS суттєво знижує ризик атак, оскільки маніпуляція мережею стає економічно невигідною. Крім того, застосування Zero-Knowledge Proofs, зокрема zk-SNARKs, сприяє конфіденційності транзакцій без компрометації безпеки.

Інтеграція блокчейну з децентралізованими файловими системами, як-от IPFS, Filecoin та Storj, є перспективним напрямом для оптимізації розподіленого зберігання даних. Аналіз свідчить, що такі гібридні рішення забезпечують баланс між продуктивністю та безпекою, мінімізуючи витрати на підтримку блокчейн-мережі.

Подальший розвиток технології блокчейн зумовлений необхідністю підвищення її ефективності, масштабованості та енергоефективності. Важливими напрямами досліджень є вдосконалення консенсусних алгоритмів, розширення функціональності смарт-контрактів, інтеграція з штучним інтелектом та Інтернетом речей, а також розробка постквантових алгоритмів криптографічного захисту. У перспективі блокчейн може суттєво змінити підходи до управління даними у фінансах, державному секторі, логістиці та медицині, сприяючи підвищенню рівня прозорості та довіри в цифрових екосистемах. Однак для його масового впровадження необхідно подолати технічні та регуляторні бар’єри, а також забезпечити ефективну інтеграцію з існуючими інформаційними системами.

Список використаних джерел

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. URL: https://bitcoin.org/bitcoin.pdf.

2. Wood, G. Ethereum: A Secure Decentralized Generalized Transaction Ledger, 2014. URL: https://ethereum.org/en/whitepaper/.

3. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform, 2015. URL: https://github.com/ethereum/wiki/wiki/White-Paper.

4. Байдак, Л. С. Технологія блокчейн: перспективи застосування у фінансовому секторі / Л. С. Байдак, В. Ю. Савченко // Фінансовий простір. – 2018. – №3 (31). – С. 76–81.

5. Шостак, І. В. Використання технології блокчейн у високонавантажених інформаційних системах / І. В. Шостак, О. С. Коваленко // Вісник Національного технічного університету України «КПІ». – 2021. – №2. – С. 95–102.

6. Benet, J. IPFS - Content Addressed, Versioned, P2P File System, 2014. URL: https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6m9GLTbpH14YPSQWGWpHQcBZoTqL.

7. Protocol Labs. Filecoin: A Decentralized Storage Network, 2017. URL: https://filecoin.io/filecoin.pdf.

8. Storj Labs. Storj: Decentralized Cloud Storage, 2018. URL: https://storj.io/whitepaper.pdf.
9. Poelstra, A. Mimblewimble, 2016. URL: https://scalingbitcoin.org/papers/mimblewimble.txt.
10. Головченко, Д. В. Використання блокчейну для розподіленого зберігання інформації / Д. В. Головченко, М. С. Лисенко // Сучасні інформаційні системи. – 2022. – №1. – С. 55–60.
11. Boneh, D., Goh, E.J., Nissim, K. Evaluating 2-DNF Formulas on Ciphertexts // Theory of Cryptography Conference (TCC). – 2005.
12. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E., Virza, M. SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge // Annual Cryptology Conference. – 2013.
13. Wood, G. Polkadot: Vision for a Heterogeneous Multi-Chain Framework, 2016. URL: https://polkadot.network/PolkaDotPaper.pdf.
14. Ethereum Foundation. Ethereum 2.0: Scaling Ethereum via Sharding and Proof-of-Stake, 2020. URL: https://ethereum.org/en/eth2/.
15. Lightning Labs. The Lightning Network: Scalable Off-Chain Instant Payments, 2016. URL: https://lightning.network/lightning-network-paper.pdf.
16. Buterin, V., Poon, J. Plasma: Scalable Autonomous Smart Contracts, . URL: https://plasma.io/plasma.pdf.
17. Protocol Labs. Zero-Knowledge Proofs and Their Applications in Blockchain, 2021. URL: https://protocol.ai/blog/zero-knowledge-proofs-and-blockchain/.
18. RSK Labs. Rootstock (RSK): Smart Contracts for Bitcoin, 2018. URL: https://www.rsk.co/whitepapers/.
19. Algorand Foundation. Algorand: A Scalable, Secure, and Decentralized Digital Currency and Smart Contract Platform, 2019. URL: https://www.algorand.com/technology.
20. Hedera Hashgraph. Hedera: The Future of Public Ledgers, 2020. URL: https://hedera.com/.
21. Семенов, П. М. Використання смарт-контрактів у високонавантажених комп'ютерних системах / П. М. Семенов, О. В. Войтенко // Інформаційні технології і системи. – 2023. – №4. – С. 112–120.
22. StarkWare Industries. zk-STARKs: Scalable, Transparent Argument of Knowledge, 2021. URL: https://starkware.co/.
23. IBM Blockchain. Blockchain for Business: A Comprehensive Guide to Enterprise Blockchain Solutions, 2022. URL: https://www.ibm.com/blockchain/.