УДК 004.67:004.62
DOI https://doi.org/10.32782/2663-5941/2024.6.2/04

Гаращук Б.В.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

МЕТОД ОПТИМІЗАЦІЇ IOT-МЕРЕЖ НА ОСНОВІ БЛОКЧЕЙН ТЕХНОЛОГІЇ З ВИКОРИСТАННЯМ ПОЛЕГШЕНОГО АЛГОРИТМУ КОНСЕНСУСУ

У статті розглядається проблема оптимізації IoT-мереж з використанням блокчейн-технології для забезпечення безпеки та підвищення ефективності в умовах обмежених ресурсів IoT пристроїв. Пропонується застосування полегшеного алгоритму консенсусу Delegated Proof of Stake (DPoS), що дозволяє зменшити навантаження на мережу порівняно з традиційними методами, такими як Proof of Work (PoW) та Proof of Stake (PoS). Запропонована архітектура включає використання локальних та публічних блокчейнів для зберігання даних, що дає змогу оптимізувати процес зберігання і обміну даними серед численних пристроїв IoT. Така комбінація технологій забезпечує ефективне управління даними в умовах високої кількості пристроїв та обмежених ресурсів. В рамках дослідження запропоновано модель мережі IoT, в якій використовуються "розумні" шлюзи для інтеграції з блокчейном, що полегшує комунікацію між пристроями з низькими обчислювальними можливостями та більш потужними вузлами консенсусу. Таким чином, блокчейн здатен забезпечити високу безпеку, захист даних від несанкціонованих змін, а також підвищену пропускну здатність завдяки розподіленій архітектурі. Експериментальні результати показують, що DPoS демонструє значно кращу продуктивність, зокрема меншу затримку (менше 1 мс) та вищу пропускну здатність у порівнянні з PoS. Це робить запропоновану систему ефективною для застосувань у сфері IoT, де необхідні низька затримка, ефективне використання обмежених ресурсів та масштабованість. Використання DPoS дозволяє досягти значної економії енергоресурсів, знижує витрати на обробку даних і покращує масштабованість системи, що робить її оптимальним вибором для широкого застосування в таких галузях, як фінанси, охорона здоров'я, енергетика та інші важливі сфери, де критично важливо зберігати безпеку та конфіденційність, одночасно зберігаючи високу продуктивність і ефективність.

Ключові слова: *блокчейн, алгоритм консенсусу, IoT, смарт-контракт, DPoS.*

Постановка проблеми. Масштабованість IoT пристроїв, стабільно зростає, з кожним роком і до 2030, згідно з дослідженнями може сягнути близько 30 мільярдів девайсів [1]. Їх економічна дешевизна та підтримка сучасних інформаційних технологій, зробило масове використання IoT мереж в різних галузях, таких як охорона здоров'я, «розумні будинки», промисловість, енергетичні мережі і т.д. [8].

Більшість систем що вже впроваджені, та створюються зараз, традиційно створені на основі централізованої інфраструктури. Основною характеристикою цього підходу є, те що дані збирають і обробляються через центральний сервер.

Такий підхід має ризики пов'язані з безпекою та конфіденційністю через можливі кібератаки [2; 6]. Застосування блокчейну є ефективним рішення для забезпечення безпеки мереж IoT. Блокчейн – цифровий розподілений реєстр, використовуючи децентралізацію та криптографічні алгоритми для захисту, він може забезпечити безпеку IoT пристроїв [2]. Блокчейн створюючи ланцюги блоків, унеможливлює підміну даних, оскільки в наступному блоці записується хеш попереднього, для змінення даних потрібно змінювати кожен блок.

Децентралізована природа блокчейну також сприяє підвищенню стійкості мережі до збоїв та атак. Оскільки копії реєстру зберігаються на багатьох вузлах мережі, відмова одного або кількох вузлів не впливає на загальну працездатність системи. Крім того, будь-які спроби несанкціонованої зміни даних можуть бути легко виявлені іншими учасниками мережі.У контексті IoT мереж, інтеграція блокчейну може забезпечити безпечну та ефективну передачу даних між пристроями без необхідності довіряти центральному вузлу. Це дозволяє знизити ризики, пов'язані з централізацією, та забезпечити вищий рівень безпеки та конфіденційності.

Однак, застосування блокчейну в IoT також має свої виклики. Одним з основних є масштабованість блокчейн мережі, оскільки збільшення

кількості транзакцій може призвести до затримок та зростання витрат на обробку. Також важливо враховувати обмежені ресурси IoT пристроїв, такі як енергія та обчислювальна потужність, які можуть бути достатніми для роботи з деякими блокчейн протоколами.

Для подолання цих викликів розробляються спеціалізовані блокчейн рішення, оптимізовані для IoT. Вони включають використання легких консенсусних алгоритмів, які потребують менше ресурсів, та впровадження механізмів, що дозволяють зменшити навантаження на мережу.У підсумку, блокчейн має потенціал значно покращити безпеку та ефективність IoT мереж, проте для повного розкриття цього потенціалу необхідно продовжувати дослідження та розробку технологій, що враховують специфічні вимоги та обмеження IoT середовища.

Аналіз останніх досліджень і публікацій. Зі зростанням популярності блокчейну технологія стикається з проблемою масштабування, особливо коли мова йде про зберігання та обробку великих обсягів даних. Це призводить до зниження продуктивності системи, оскільки мережа, що перевіряє транзакції, стає більш складною і не здатна обробляти велику кількість транзакцій одночасно. Це особливо актуально для алгоритмів консенсусу, таких як Proof of Work (PoW) та Proof of Stake (PoS), які мають обмежену пропускну здатність і можуть створювати вузькі місця в мережі.

Алгоритм консенсусу – це набір правил та протоколів, за допомогою яких учасники блокчейн-мережі досягають згоди щодо поточного стану системи та історії її транзакцій. Основними функціями алгоритму консенсусу є:

1. Перевірка транзакцій: Забезпечення того, щоб всі транзакції в мережі були дійсними та відповідали встановленим правилам. Це включає перевірку підписів, балансу та відсутності подвійного витрачання.

2. Додавання нових блоків: Визначення механізму, за яким нові блоки додаються до ланцюга, коли з'являються нові транзакції. Алгоритм визначає, який учасник має право додати наступний блок, та як це рішення приймається.

3. Управління відмовами та конфліктами: Якщо виникають конфлікти або різні учасники мають різну інформацію, консенсусний алгоритм визначає, яка з версій є правильною, забезпечуючи цілісність та послідовність блокчейну.

Основними алгоритмами консенсусу є Proof of Work та Proof of Stake. Розглянемо детальніше кожен з них, їхні переваги та недоліки.

Proof of Work (PoW) – це перший і найпоширеніший алгоритм консенсусу, який використовується в багатьох блокчейн-мережах, включаючи Bitcoin [2]. Учасники мережі, відомі як майнери, повинні виконувати складні обчислювальні задачі для того, щоб додати новий блок до блокчейну [4]. Ці задачі зазвичай включають пошук хешу з певними властивостями, що відповідає вимогам мережі. Майнери змагаються між собою, щоб першим знайти правильне рішення, і той, хто успішно вирішує задачу, отримує винагороду у вигляді криптовалюти.

Переваги PoW:

– Високий рівень безпеки: Завдяки складним обчисленням і необхідності виконання великої кількості операцій для додавання кожного блоку, PoW робить систему захищеною від атак. Зокрема, для того щоб зловмисник зміг змінити історію транзакцій, йому потрібно мати більше 50% обчислювальної потужності мережі, що є вкрай складним завданням.

– Децентралізація: Усі учасники можуть брати участь у процесі майнінгу, що підтримує децентралізований характер мережі. Це забезпечує відсутність єдиного центру контролю та підвищує стійкість до цензури.

Недоліки PoW:

– Високі витрати на енергію та обчислювальні ресурси: Для обробки транзакцій та додавання нових блоків потрібен великий обсяг енергії. Це призводить до значних екологічних проблем та збільшує витрати на підтримку мережі.

– Масштабованість: Час на створення нового блоку в PoW може бути великим (наприклад, 10 хвилин у Bitcoin), що обмежує кількість транзакцій, які можуть бути оброблені за секунду. Це робить систему менш ефективною для використання в масштабних проектах, де необхідна висока пропускна здатність.

Proof of Stake (PoS) – це альтернативний алгоритм консенсусу, який замінює обчислювальні завдання PoW на принцип володіння часткою в мережі. У PoS учасники, які мають більше токенів або «ставок» (stakes), мають більший шанс бути вибраними для перевірки транзакцій і додавання нових блоків до блокчейну. Це означає, що стимул для підтримки мережі базується на власності токенів, а не на обчислювальній потужності.

Переваги PoS:

– Масштабованість: PoS дозволяє значно швидше додавати нові блоки до блокчейну, що збільшує пропускну здатність мережі. Це робить її більш придатною для додатків, де необхідна швидка обробка великої кількості транзакцій.

– Безпечність: Зловмисник повинен володіти значною кількістю токенів, щоб здійснити атаку на систему, що робить такі атаки економічно невигідними. Це підвищує загальну безпеку мережі.

– Енергоефективність: Оскільки немає потреби у виконанні складних обчислень, енергоспоживання мережі значно знижується, що позитивно впливає на екологію та зменшує витрати.

Недоліки PoS:

– Ризик концентрації влади: Якщо одна особа чи група володіє більшістю монет, вони можуть отримати не пропорційну кількість голосів для валідації блоків, що може призвести до централізації. Це суперечить основному принципу децентралізації блокчейну.

– Менша перевіреність: У порівнянні з PoW, PoS є новішим алгоритмом, і деякі експерти вважають його менш перевіреним на практиці. Існують побоювання щодо потенційних вразливостей та стабільності системи в довгостроковій перспективі.

Значні обчислювальні вимоги цих алгоритмів, особливо в PoW, роблять їх не практичними для IoT пристроїв з обмеженими ресурсами [5][7]. Більшість IoT-пристроїв мають обмежену обчислювальну потужність, пам'ять та енергетичні ресурси, що унеможливлює ефективне використання цих алгоритмів без шкоди для їх основних функцій.

Тому наш метод використовує альтернативний консенсус, відомий як Delegated Proof of Stake (DPoS). У цьому алгоритмі лише обрана кількість делегатів перевіряє транзакції та додає блоки. Учасники мережі голосують за делегатів, які представлятимуть їх інтереси в процесі валідації блоків. Це дозволяє збільшити швидкість обробки транзакцій та знизити навантаження на мережу.

Переваги DPoS:

– Висока продуктивність: Зменшення кількості вузлів, які беруть участь у консенсусі, дозволяє значно збільшити швидкість підтвердження транзакцій та додавання нових блоків. Це особливо важливо для мереж з великою кількістю транзакцій.

– Енергоефективність: Оскільки тільки вибрані делегати виконують обробку транзакцій, загальне енергоспоживання мережі знижується. Це робить DPoS більш придатним для пристроїв з обмеженими ресурсами, таких як IoT.

– Гнучкість: Учасники мережі можуть легко змінювати делегатів через механізм голосування, що забезпечує адаптивність та стійкість до зловживань з боку делегатів.

DPoS є більш підходящим для IoT-пристроїв завдяки своїй енергоефективності та швидкості. Оскільки IoT-пристрої часто мають обмежені ресурси та потребують швидкої обробки даних, DPoS забезпечує необхідний баланс між безпекою та продуктивністю.

У DPoS IoT-пристрої можуть діяти як звичайні учасники, делегуючи свої права перевірки транзакцій більш потужним вузлам. Це дозволяє знизити вимоги до обчислювальних ресурсів та енергії на самих пристроях, що є критичним для їхнього функціонування.

Переваги DPoS для IoT:

– Зменшення навантаження: Пристрої не повинні виконувати складні обчислення, що продовжує їхній термін роботи від батареї та зменшує знос обладнання.

– Швидкість транзакцій: Підвищена швидкість обробки транзакцій дозволяє в реальному часі реагувати на події та зміни, що важливо для багатьох IoT-застосувань.

– Масштабованість: DPoS може підтримувати велику кількість пристроїв та транзакцій без значного зниження продуктивності мережі.

Проблеми масштабування та продуктивності є серйозними перешкодами для інтеграції блокчейну в IoT-системи. Традиційні алгоритми консенсусу, такі як PoW та PoS, не відповідають вимогам IoT-пристроїв через високі обчислювальні вимоги та енергоспоживання. Використання альтернативного алгоритму консенсусу DPoS пропонує ефективне рішення цих проблем.

DPoS забезпечує необхідну продуктивність та енергоефективність, дозволяючи IoT-пристроям взаємодіяти з блокчейн-мережею без перевищення їхніх ресурсних можливостей. Хоча існують ризики, пов'язані з централізацією та залежністю від голосування, правильне налаштування та активна участь спільноти можуть мінімізувати ці недоліки.

Таким чином, DPoS представляє собою перспективний напрямок розвитку блокчейн-технологій для IoT, що може значно покращити безпеку, продуктивність та масштабованість мереж, відкриваючи нові можливості для інновацій та інтеграції в різних галузях.

Постановка завдання. Метою даної статті є аналіз існуючих підходів до використання блокчейну та алгоритмів консенсусу в IoT мережах, виявлення основних недоліків і моделювання архітектури системи з використанням полегшеного консенсусу, яка підвищує безпеку та продуктивність в умовах обмежених ресурсів IoT пристроїв.

Виклад основного матеріалу. Запропонована система організована таким чином, що IoT

пристрої використовують, для взаємодії з блокчейном, «розумні» шлюзи. Вони допомогають подолати розрив між обмеженими можливостями пристроїв і смарт контрактами блокчейну. Також ми використовуємо. IoT вузли збирають дані та надсилають їх до локального блокчейну на визначених користувачем інтервалах. А вузли консенсусу, ще крім збору даних, також використовують алгоритм консенсусу DPoS. Обидва види вузлів, не мають потреби у високих обчислювальних вимогах завдяки застосованому консенсусу.

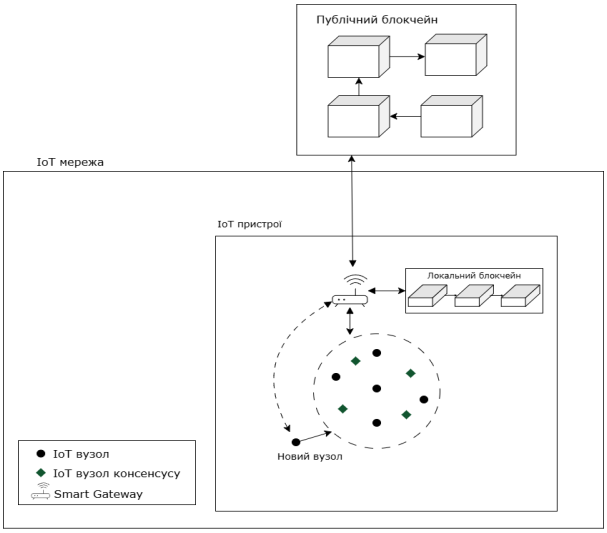

Рис. 1. Архітектура запропонованої системи

Коли новий вузол хоче приєднатись до мережі, шлюз полегшує комунікацію з вузлами консенсусу. З доступного набору вузлів обирається валідатор, котрий визначається за його обчислювальною потужністю та функціонуванням.

Використовуючи подвійну блокчейн-систему, що складається з локального блокчейну та публічного блокчейну, спеціально розробленого для обмежених IoT пристроїв. Локальний блокчейн тимчасово зберігає всі IoT дані, функціонуючи як буфер, що містить хеш-адреси та ідентифікаційні реєстри, які вказують на місця зберігання даних у публічному блокчейні, що виступає як централізований реєстр. Публічний блокчейн таким чином слугує постійним сховищем для усього потоку IoT даних, що передаються через всю IoT інфраструктуру.

Публічний блокчейн функціонує як децентралізована мережа, що складається з окремих вузлів, кожен з яких містить повну копію всієї системи. Такий підхід забезпечує стійкість системи, навіть якщо значна частина вузлів мережі стає недоступною або втрачаються дані. У таких випадках систему можна повністю відновити, використовуючи лише один вузол із повною копією блокчейну.

Оцінка ефективності, складається з кількох етапів, таких як валідація додавання даних до блоку та вимірювання пропускної здатності.

Затримка – показує час який потрібен для того щоб пакет досягнув шлюзу та став частиною блокчейну. Чим вище показник тим більша складність додавання пакеті даних до блоку.

Тестові налаштування були такими, загальна кількість вузлів від 500 до приблизно 2000. Розмір блоку, що вміщує пакети даних – 1МБ, а розмір корисного навантаження – 50 Байт. Рисунок 2 демонструє результати. При застосування алгоритму PoS, затримка зростала. Наприклад, для 500 вузлів, у консенсусу PoS затримка складає – 50 мс, в той же час DPoS демонструє близько 1 мс. Пояснити це можна тим, що у PoS – процес валідації для окремого пакету даних затягнутий через відсутність миттєвого виконання та більший пул валідації. В результаті ці пакети даних ставляться в чергу на валідацію та подальше додавання до блоків.

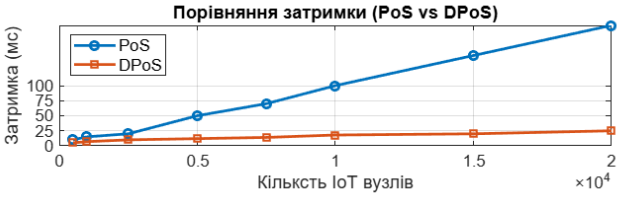

Рис. 2. Порівняння часу затримки між системами з PoS та DpoS

Пропускна здатність – вимірюється кількістю успішних транзакцій від першої транзакції до останньої в ланцюзі блоків. Показує кількість вузлів IoT блокчейну на шлюз. З результатами можна ознайомитись на рисунку 3. В цьому випадку різницю можна пояснити, тим підхід PoS насичується раніше, не досягаючи більш високої пропускної здатності.

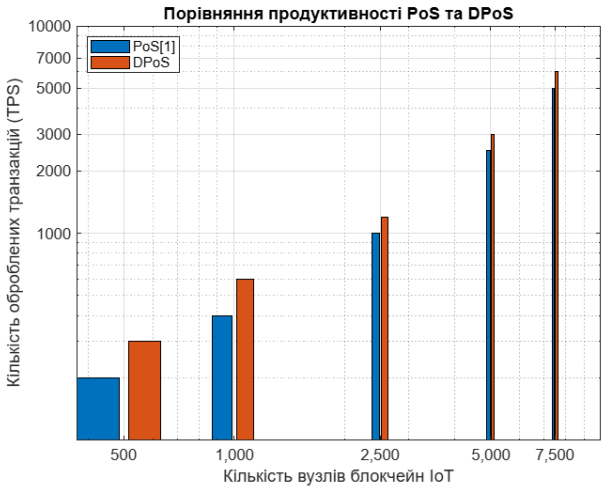

Рис. 3. Порівняння пропускної здатності системами з PoS та DpoS

Висновки. Таким чином, запропонована система досягає кінцевої безпеки через механізми верифікації та валідації, що залучають обраних делегатів, щоб зменшити проблеми з деградацією продуктивності на пристроях. Експериментальні результати показують, що DPoS перевершує PoS за показниками пропускної здатності та латентності на пристроях IoT. Ми також демонструємо, що підхід DPoS корисний для застосувань IoT, де необхідніа ефективне використання ресурсів. Завдяки цим показникам рішення може бути застосовано у фінансовій та медичній галузях. Крім того, низька вартість є критично важливою для широкого впровадження блокчейн-технологій для безпечного управління та зберігання даних у середніх та великих організаціях.

Список літератури:

1. Holst A. IoT Connected Devices Worldwide 2022–2030 Statista. 2024. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (дата звернення: 15.11.2024).

2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. – 2008. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 17.11.2024).

3. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper 2013. URL: https://ethereum.org/en/whitepaper/ (дата звернення: 18.11.2024).

4. Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Alan Colman. Blockchain Consensus Algorithms: A Survey. arXiv. – 2020.Pp. 1–32. URL: https://arxiv.org/abs/2001.07091 (дата звернення: 19.11.2024).

5. Larimer D. Delegated Proof-of-Stake (DPoS). BitShares 2014. URL: https://bitshares.org/technology/delegated-proof-of-stake-consensus/ (дата звернення: 19.11.2024).

6. Mollah S.M., Azad M.A.K., Vasilakos A.V. Comparison of PoS and DPoS Consensus Algorithms in Blockchain. Journal of Electrical Engineering and Technology. 2020 Vol. 15, No. 6. Pp. 3067–3074. URL: https://doi.org/10.1007/s42835-020-00536-0 (дата звернення: 19.11.2024).

7. Chan S.C.Y., Chow K.P., Wong D.S., et al. Blockchain for Internet of Things: A Survey // IEEE Internet of Things Journal 2019. Vol. 6, No. 5. Pp. 8076–8094. URL: https://ieeexplore.ieee.org/document/8731639 (дата звернення: 20.11.2024).

8. Li R.Y.K., Chau K.W., Tsai C.W., et al. A Hybrid Blockchain Architecture for Secure IoT Communication. Future Generation Computer Systems. 2019. Vol. 96. Pp. 481–489. URL: https://doi.org/10.1016/j.future.2019.02.049 (дата звернення: 20.11.2024).

Garashchuk B.V. A METHOD FOR OPTIMIZING IoT NETWORKS BASED ON BLOCKCHAIN TECHNOLOGY USING A LIGHTENED CONSENSUS ALGORITHM

The article considers the problem of optimizing IoT networks using blockchain technology to ensure security and increase efficiency in the context of limited resources of IoT devices. The paper proposes the use of a lightweight Delegated Proof of Stake (DPoS) consensus algorithm that reduces the load on the network compared to traditional methods such as Proof of Work (PoW) and Proof of Stake (PoS). The proposed architecture includes the use of local and public blockchains for data storage, which allows optimizing the process of storing and exchanging data among numerous IoT devices. This combination of technologies ensures efficient data management in the context of a high number of devices and limited resources. The study proposes a model of the IoT network that uses smart gateways to integrate with the blockchain, which facilitates communication between devices with low computing capabilities and more powerful consensus nodes. Thus, the blockchain is able to provide high security, data protection against unauthorized changes, and increased throughput due to its distributed architecture. Experimental results show that DPoS demonstrates significantly better performance, including lower latency (less than 1 ms) and higher throughput compared to PoS. This makes the proposed system effective for IoT applications that require low latency, efficient use of limited resources, and scalability. The use of DPoS allows for significant energy savings, reduces data processing costs, and improves system scalability, making it the optimal choice for widespread use in industries such as finance, healthcare, energy, and other critical areas where it is critical to maintain security and privacy while maintaining high performance and efficiency.

Key words: *blockchain, consensus algorithm, IoT, smart contract, DPoS.*