DOI: https://doi.org/10.15276/ict.02.2025.26
УДК 004.75:004.56

Можливість використання концепції динамічного кластерингу блокчейн-системи Proof-of-Work для вдосконалення систем державного управління

Соловйова Діана Вячеславівна [1)]
Асистент каф. Інформаційних систем
ORCID: https://orcid.org/0009-0007-5253-8848; soloviova.d.v@op.edu.ua. Scopus Author ID: 59185442400
Болтьонков Віктор Олексійович [1)]
Канд. техніч. наук, доцент каф. Інформаційних систем
ORCID: https://orcid.org/0000-0003-2777-3137; vaboltenkov@gmail.com. Scopus Author ID: 57203623617
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Сучасне державне управління стикається з численними викликами, такими як корупція, бюрократичні затримки, неефективне використання ресурсів та низький рівень довіри громадян. Одним із перспективних шляхів підвищення ефективності та прозорості державних процесів є цифровізація та впровадження блокчейн-технологій. Блокчейн забезпечує децентралізацію, прозорість та незмінність даних, що дозволяє зменшити ризики корупції та спростити міжвідомчу взаємодію, аналіз міжнародного досвіду показує ефективність використання блокчейну в державних системах.

Класичний механізм консенсусу Proof-of-Work (PoW), що залишається еталоном децентралізації та доведеної безпеки, має суттєві обмеження для його використання у сфері державного управління: високе енергоспоживання та низьку пропускна здатність у пікові періоди. У роботі запропоновано модифіковану методику динамічного кластерування вузлів у PoW-мережах для державного сектору, що дозволяє об'єднувати вузли в кластери з інтенсивним внутрішнім обміном та використовувати локальний PoW для швидкої обробки транзакцій. Для досягнення фінального консенсусу на національному рівні застосовується протокол PBFT, що забезпечує стійкість до візантійських збоїв та детерміновану фінальність. Математична модель підтверджує, що оптимізація розміру кластерів та комбінування PoW і PBFT дозволяє зменшити час підтвердження транзакцій, підвищити пропускну здатність системи та значно знизити енергоспоживання. Додатково запроваджується періодична перекоммутація вузлів між кластерами, що підвищує стійкість до 51%-атаки.

Запропонована гібридна архітектура PoW+PBFT демонструє баланс між децентралізованою безпекою, продуктивністю та енергоефективністю. Методика має сенс для впровадження в масштабних державних сервісах, таких як електронне голосування, державні реєстри, публічні закупівлі та соціальні виплати, забезпечуючи прозорість, швидкість та надійність обробки транзакцій.

Ключові слова: блокчейн; Proof-of-Work; динамічне кластерування; державне управління; PBFT; електронне урядування; енергоефективність; безпека транзакцій; державні реєстри; цифровізація

Актуальність. Державне управління в сучасному світі стикається з проблемами корупції, бюрократичних затримок, неефективного використання ресурсів та низької довіри громадян. Тому по-перше, ця проблема є актуальною, а по-друге, найбільш сучасним та практичним підходом до її вирішення є цифровізація процесів у державному управлінні, його цифрова трансформація.

В свою чергу цифрова трансформація державного управління формулює чіткі та жорсткі виклики та вимагає створення абсолютно прозорих, надійних та масштабованих інформаційних систем, здатних обробляти великі обсяги даних у режимі реального часу. У цьому контексті варто згадати про технологію блокчейну, що постає перед нами як надійний інструмент формування довіреного та незмінного реєстру – забезпечує відкритість процесів, зменшує ризики корупції та спрощує міжвідомчу взаємодію. Блокчейн-технології пропонують рішення через децентралізацію, прозорість та незмінність даних, що може революціонізувати електронне урядування. Згідно з аналізом [1], блокчейн вже інтегрується в державні функції для підвищення ефективності та довіри, наприклад, у реєстрації майна та виборах.

Тому дана робота присвячена дослідженню впровадження технології блокчейну у процеси державного управління.

Іноземні джерела підкреслюють реальне застосування блокчейну в публічному секторі [2], такі як естонська система охорони здоров'я та грузинський реєстр землі. Естонія

використовує блокчейн у e-Residency для захисту даних, інтегруючи з X-Road для міжвідомчого обміну (99 % послуг оцифровано). Грузія впровадила реєстр нерухомості, зареєструвавши 1.5 млн титулів за 3 хвилини [3]. Аналізуючи особливості імплементування технологій та консенсусні механізми, можна побачити, що у держсистемах переважають приватні/гібридні блокчейни з PoS або PBFT для контролю, оскільки PoW виявляється надто енергоємним (наприклад, гібрид Ethereum-Hyperledger в Арагоні, Іспанія) [4].

Проте класичний механізм консенсусу Proof-of-Work (PoW), на якому працюють найвідоміші блокчейн-мережі, не втрачає своїх абсолютних переваг та залишається еталоном децентралізації та доведеної безпеки [5]. Для державних додатків, де першорядними є довіра, стійкість та юридична прозорість, модифікований PoW може дати реальне зниження енергоспоживання та затримок, збереження ключових переваг класичного PoW та адаптацію під масштабні національні сервіси. Саме тому дослідження його оптимізації, а не відмова на користь PoS/PoA виправдане і науково, і стратегічно.

Отже, **метою дослідження** є обґрунтування можливості впровадження методу динамічного кластерування вузлів у мережах PoW для потреб державного сектору. Такий підхід покликаний підвищити швидкість підтвердження транзакцій та загальну масштабованість державних блокчейн-сервісів (електронне голосування, ведення реєстрів, соціальні виплати), зберігаючи при цьому ключові переваги децентралізованої та прозорої архітектури.

Говорячи про впровадження системи блокчейну, класичний механізм PoW має суттєві недоліки: низьку пропускну здатність, що ускладнює обробку великої кількості транзакцій під час пікових навантажень, та високе енергоспоживання, яке створює додаткові фінансові та екологічні витрати. Тому розглянемо методику, що розроблювалася авторами даної роботи [6], що передбачає моделювання мережі із реалізацією динамічного розбиття системи блокчейну із механізмом консенсусу Proof-of-Work на кластери, використовуючи K-means та OPTICS за потужністю вузлів [7], враховуючи динаміку PoW (конкуренція майнерів), що направлена на вирішення вище згаданих проблем.

Запропонований підхід базується на динамічному розбитті мережі на кластери, де вузли об’єднуються в групи з інтенсивним внутрішнім обміном.

Експериментальне моделювання продемонструвало покращення ключових показників:

– пропускна здатність (TPS) зросла приблизно на 0,02 транзакції/с,
– середній час підтвердження транзакції скоротився на 1,67 с,
– енергоспоживання зменшено на 5122 умовних одиниці для обробки 30 транзакцій.

Витрачену системою енергію було розраховано наступним чином, тому через перевагу у часі та потужності, отримано перевагу у енергоспоживанні:

$$E = (t_{\text{майн.}} + t_{\text{сінх.}}) * \text{P}, \quad (1)$$

де E – затрачена системою енергія,

$t_{майн.}$ – час, затрачений на майнінг у системі,

$t_{сінх.}$ – час, затрачений на синхронізацію вузлів, передачу сигналу про закінчення майнінгу до всіх вузлів системи (прийняття консенсусу),

P – загальна потужність системи.

Основним обмеженням методикі стала підвищена вразливість до атаки 51% при збільшенні кількості кластерів: із зменшенням розміру кожного кластера спадає сумарна обчислювальна потужність, необхідна для його компрометації. Рівень безпеки системи безпосередньо залежить від кількості кластерів та рівня складності системи та розраховується наступним чином:

$$S = \frac{O^2}{\sqrt{N}}, \quad (2)$$

де S – рівень безпеки системи,

O – складність системи,

N – кількість кластерів у мережі.

Проаналізувавши переваги та недоліки розробленої методики, було встановлено, що використання у держсекторі базовий метод слід доповнити гібридним консенсусом, щоб зберегти децентралізовану безпеку PoW, але усунути вразливість до 51 %-атаки та зберегти перевагу зменшеного енергоспоживання.

Отже, пропонується наступна архітектура моделі. Мережа поділяється на кластери C_i розміром n_i вузлів. Усередині кожного кластера PoW використовується лише для генерації «робочого доказу» блоку та швидкої локальної перевірки. Після внутрішньої валідації представники кластерів («лідери») беруть участь у протоколі Practical Byzantine Fault Tolerance (PBFT) для досягнення фінальної згоди на загальнодержавному рівні.

Вибір протоколу PBFT як верхнього рівня консенсусу обґрунтований його здатністю забезпечувати швидку фінальність транзакцій та стійкість до візантійських збоїв за умови наявності обмеженої кількості довірених учасників (лідерів кластерів) [9]. У моделі державного управління кількість лідерів відома й контрольована (сертифіковані дата-центри або муніципальні вузли), що відповідає передумовам PBFT: протокол гарантує коректність при наявності не більше ніж $f < \frac{n}{3}$ зловмисних вузлів та забезпечує детерміновану фінальність без повторного підтвердження, на відміну від PoW чи PoS, де можливі реорганізації ланцюга [10].

Візуалізуємо архітектуру гібридного блокчейн-рішення, яку можна використовувати для державного управління (рис. 1).

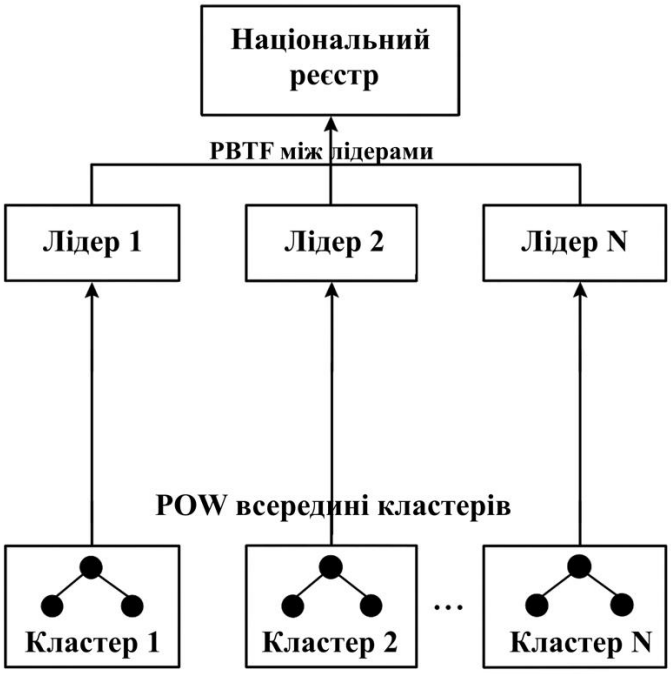

Рис. 1. **Архітектура гібрідного блокчейн-рішення для державного управління**

Роздивимося схему. Нижній рівень, кластери — це групи вузлів мережі (ноди громадян, організацій, дата-центрів), причому усередині кожного кластера транзакції обробляються за механізмом PoW. Їх завдання – швидко формувати та перевіряти блоки, мінімізуючи затримки за рахунок локальної синхронізації.

Середній рівень – це лідери кластерів, по одному представнику (лідеру) кожного кластера. Лідери можуть бути державними чи сертифікованими муніципальними дата-центрами, вони збирають Merkle-root блоків своїх кластерів, беруть участь у протоколі PBFT задля досягнення фінального консенсусу. З використанням лідерів тепер, щоб атакувати систему, зловмисникові недостатньо захопити один кластер – треба також отримати контроль над більшістю лідерів.

Верхній рівень, національний реєстр – загальнодержавний ланцюжок блоків, до якого входять блоки, підтверджені більшістю лідерів, що виконує функцію зберігання фінальної версії даних (реєстр нерухомості, результати голосування).

Отже, за схемою транзакції приходять у кластери та валідуються по PoW – тут створюється локальний блок. Лідери збирають хеші цих блоків та обмінюються ними через PBFT та досягають фінальності. Потім національний реєстр приймає блок лише після згоди ≥ 2/3 лідерів. В цьому випадку PoW залишається лише на локальному рівні, тому затримка підтвердження зменшується, немає потреби у глобальному «майнінгу» всією мережею, що корисно для енергоефективності та тут комбінуються два бар'єри – обчислювальна складність PoW у кластерах та візантійська стійкість PBFT на рівні лідерів. Фіналізуючи пояснене вище, взаємодії між вузлами системи відобразимо на рис. 2.

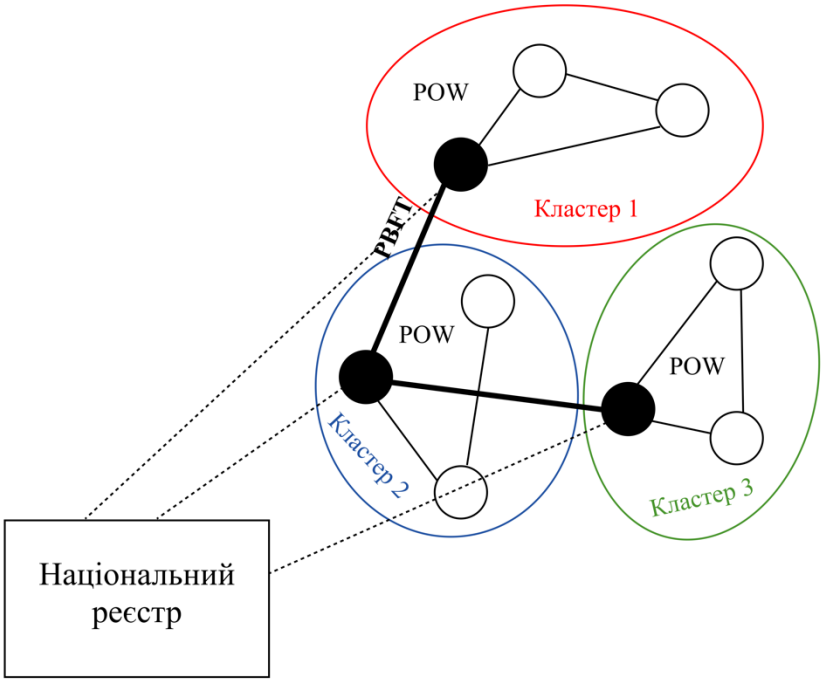

Рис.2. **Схема кластеризації гібридної мережі**

На рис. 2 маленькими колами позначено кожен окремий вузол мережі (громадяни, організації, дата-центри). Кола або еліпси, що об'єднують кілька вузлів, позначають кластери, всередині яких використовується PoW для локального майнінгу. Виділені вузли всередині кластера (темні кола) – лідери кластерів, які беруть участь у PBFT на глобальному рівні. Тонкі лінії між вузлами всередині кластера показують інтенсивний обмін даними, а товстіші лінії між лідерами, що показують консенсус PBFT, є зв'язками між кластерами. І відповідно, верхній рівень, прямокутник, куди агрегуються дані з лідерів – це національний реєстр.

Наступним кроком пишемо математично модель гібридного консенсусу PoW+PBFT. Нехай час поширення блоку в кластері – t_{cl}, міжкластерна синхронізація – t_{net}. Тоді загальний час підтвердження транзакції:

$$T_{tx} = t_{cl}^{POW} + t_{agg}^{PBFT} + t_{net}, \tag{3}$$

де t_{agg}^{PBFT} – час досягнення консенсусу лідерів.

За умови оптимізації розміру кластера (мінімізація функції $f(n_i) = t_{cl}(n_i) + t_{agg}(n_i)$) маємо:

$$T_{tx} \approx O(\log n_i) + O(k), \tag{4}$$

де k – кількість кластерів, що дає суттєве скорочення порівняно з класичним PoW, де затримка пропорційна розміру всієї мережі.

Отже, для компрометації системи зловмиснику тепер необхідно не лише контролювати ≥ 51 % хешрейту в окремому кластері, а й отримати $\geq \frac{2}{3}$ голосів лідерів у PBFT, що значно підвищує поріг атаки. Додатково впроваджується періодична перекоммутація вузлів між кластерами за випадковим детермінованим алгоритмом R(t), що зменшує ризик довготривалого захоплення окремого кластера.

Роздивимося практичну реалізацію запропонованою методикою. Керування кластерами відбувається таким чином, що лідерами обираються дата-центри або вузли, що пройшли державну сертифікацію; при цьому участь у PoW може брати будь-який громадянин або організація. Щодо криптографічних гарантій, для підтвердження коректності внутрішньої синхронізації кожен кластер публікує агрегований Merkle-root свого міні-ланцюга, підписаний лідером, який перевіряється на рівні PBFT. Зберігання персональних даних організовується у зашифрованому вигляді з дотриманням GDPR та національного законодавства.

Таким чином, поєднання динамічного кластерування з гібридним консенсусом зберігає ключові переваги PoW (децентралізація, перевірена безпека), скорочує середній час транзакції за рахунок локальної обробки, та істотно підвищує стійкість до 51 %-атаки, оскільки для її проведення необхідно одночасно зламати PoW-частину й перевищити поріг PBFT. Тому модифікована методика стає придатною для масштабних державних сервісів, забезпечуючи баланс між надійністю, продуктивністю та вимогами енергоефективності.

Запропонована методика покращеного механізму консенсусу PoW із кластеризацією має такі цільові сфери державного управління як:

– електронне голосування – швидке підрахування бюлетенів у періоди пікового навантаження;

– державні реєстри землі й нерухомості – пришвидшена реєстрація та оновлення прав власності;

– публічні закупівлі та тендери – миттєва фіксація заявок і контрактів, що знижує корупційні ризики;

– соціальні виплати та субсидії – масова обробка транзакцій з мінімальною затримкою.

Отже, використання методики динамічного кластерування вузлів у PoW-мережах дозволяє підвищити пропускну здатність та скоротити час підтвердження транзакцій у державних системах. Проте для забезпечення збереження децентралізованої безпеки та стійкість до візантійських збоїв і 51%-атак запропоновано використання гібридного консенсусу PoW+PBFT, де локальний PoW у кластерах зменшує глобальне енергоспоживання та дозволяє масштабувати систему для пікових навантажень.

Запропонована методика має сенс для реалізації у ключових сферах державного управління: електронне голосування, державні реєстри, публічні закупівлі, соціальні виплати, що буде описано авторами детальніше у подальших дослідженнях на цю тему. Поєднання динамічного кластерування з гібридним консенсусом забезпечує баланс між надійністю, продуктивністю та енергоефективністю, що робить систему придатною для національного рівня.

СПИСОК ЛІТЕРАТУРИ

1. Lee N. T., Wang J. “Governments are turning to blockchain for public good–here’s how”. *The Brookings Institution.* 2025. – URL: https://www.brookings.edu/articles/governments-are-turning-to-blockchain-for-public-good-heres-how.

2. “Global case studies: Blockchain initiatives in the public sector”. *BlockApps.* – URL: https://blockapps.net/blog/global-case-studies-blockchain-initiatives-in-the-public-sector.

3. “Analyzing the role of blockchain technology in strengthening democracies”. *Center for Strategic and International Studies.* – URL: https://www.csis.org/analysis/analyzing-role-blockchain-technology-strengthening-democracies.

4. Zohar M., et al. “Blockchain-based solutions for public sector challenges”. *Frontiers in Blockchain.* 2022; 5: 869665. DOI: https://doi.org/10.3389/fbloc.2022.869665.

5. Arslan M., et al. “Comparative analysis and modern applications of PoW, PoS, PPoS blockchain consensus mechanisms and new distributed ledger technologie”. 2021.

6. Soloviova D., Antoshchuk S., Boltenkov V. “Research into the possibilities of improving Proof-of-Work blockchain technology”. *Herald of Advanced Information Technology.* 2021; 7: 131–146. DOI: https://doi.org/10.15276/hait.07.2021.6.

7. Qin J., Fu W. “Distributed k-means algorithm and fuzzy c-means algorithm for sensor networks based on multiagent consensus theory”. *IEEE Transactions on Cybernetics*. 2017; 47 (3): 772–783. DOI: https://doi.org/10.1109/TCYB.2016.2571460.

8. Zheng Z., et al. “Blockchain challenges and opportunities: A survey”. *International Journal of Web and Grid Services.* 2018; 14 (3): 352–375. DOI: https://doi.org/10.1504/IJWGS.2018.10015376.

9. Androulaki E., et al. “Hyperledger Fabric: A distributed operating system for permissioned blockchains”. *EuroSys.* 2018. DOI: https://doi.org/10.1145/3190508.3190538.

DOI: https://doi.org/10.15276/ict.02.2025.26
UDC 004.75:004.56

The possibility of using the concept of dynamic clustering of the Proof-of-Work blockchain system to improve public administration systems

Diana V. Soloviova[1)]
Assistant of the Department Information Systems
ORCID: https://orcid.org/0009-0007-5253-8848; soloviova.d.v@op.edu.ua. Scopus Author ID: 59185442400
Viktor O. Boltenkov[1)]
PhD, Associate Professor of the Department Information Systems
ORCID: https://orcid.org/0000-0003-2777-3137; vaboltenkov@gmail.com. Scopus Author ID: 57203623617
[1)] Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine

ABSTRACT

Modern public administration faces numerous challenges, such as corruption, bureaucratic delays, inefficient use of resources and low level of trust of citizens. One of the promising ways to increase the efficiency and transparency of public processes is digitalization and implementation of blockchain technologies. Blockchain provides decentralization, transparency and immutability of data, which allows to reduce the risks of corruption and simplify interagency interaction, analysis of international experience shows the effectiveness of using blockchain in public systems.

The classic Proof-of-Work (PoW) consensus mechanism, which remains the benchmark of decentralization and proven security, has significant limitations for its use in the field of public administration: high energy consumption and low throughput during peak periods. The paper proposes a modified method of dynamic clustering of nodes in PoW networks for the public sector, which allows combining nodes into clusters with intensive internal exchange and using local PoW for fast transaction processing. To achieve the final consensus at the national level, the PBFT protocol is used, which provides resistance to Byzantine faults and deterministic finality. The mathematical model confirms that optimizing the cluster size and combining PoW and PBFT allows to reduce the transaction confirmation time, increase the system throughput and significantly reduce energy consumption. In addition, periodic switching of nodes between clusters is introduced, which increases the resistance to 51% attacks. The proposed PoW+PBFT hybrid architecture demonstrates a balance between decentralized security, performance and energy efficiency. The methodology makes sense for implementation in large-scale government services, such as electronic voting, state registries, public procurement and social payments, ensuring transparency, speed and reliability of transaction processing.

Keywords: Blockchain; Proof-of-Work; dynamic clustering; public administration; PBFT; e-government; energy efficiency; transaction security; public registries; digitalization