DOI 10.15276/imms.v13.no1-2.48
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 1-2, pp.48-55

РОЗРОБКА ПЛАТФОРМИ ДЕЦЕНТРАЛІЗОВАНОГО РЕЄСТРУ З ПОКРАЩЕНИМИ ХАРАКТЕРИСТИКАМИ

С.С. Грибняк

Національний університет «Одеська Політехніка»
просп. Шевченка, 1, Одеса, 65044, Україна
e-mail: ssgrybniak@op.edu.ua

Технології розподілених реєстрів за п'ятнадцять років свого існування знайшли широке застосування у сфері фінансового обороту, криптовалютних додатках, системах захищеного документообігу. Найбільш популярними на сьогоднішній день є блокчейн системи Bitcoin та Etherium. Незважаючи на їх переваги (незмінність відпрацьованих транзакцій, децентралізованість, прозорість), вони мають серйозні недоліки – невисоку швидкість обробки транзакцій і обмежену масштабованість. У цьому плані їм складно конкурувати з централізованими фінансовими платформами, що мають швидкість обробки транзакцій на порядки вище. Мета цієї роботи – розробка платформи, на основі технології децентралізованого реєстру з покращеними характеристиками масштабованості та швидкості обробки транзакцій. В основу побудови системи покладено архітектуру, засновану на спрямованому ациклічному графі – BlockDAG, яка вигідно відрізняється від Blockchain асинхронністю функціонування. Упорядкування блоків у ній здійснюється шляхом топологічного лінійного сортування спрямованого графа. Крім того, швидкість обробки у BlockDAG зростає зі збільшенням числа користувачів. При побудові платформи запропоновано використовувати двошарову схему, яка складається з двох мереж – основної BlockDAG мережі та координаційної мережі, побудованої на основі Blockchain. В основній мережі відбувається створення блоків та розповсюдження їх по мережі. Координаційна мережа виконує функції атестації блоків та його фіналізації. Застосовано протокол консенсусу Proof of Stake. Проведено реалізацію запропонованої схеми у вигляді експериментальної платформи Waterfall, яка призначена для обслуговування транзакцій з різними токенами, включаючи NFT, обслуговування смарт-контрактів і розробки розподілених додатків. Тестування показало високу швидкість обробки транзакції у поєднанні з необхідною масштабованістю.

Ключові слова: технології розподілених реєстрів, обробка транзакцій, двошарова мережа, BlockDAG , платформа Waterfall

Вступ. Технології розподілених реєстрів (Distrsbuted Ledger Technology, DLT) [1] є вибуховою і найбільш стрімко розвиваючоюся гілкою інформаційних технологій 21-го століття. Першим поколінням практичного застосування DLT став класичний блокчейн, описаний у 2008 році, який є одноранговою піринговою децентралізованою системою обробки транзакцій. Класичний блокчейн став основою децентралізованого фінансового обороту і першої криптовалюти – біткойн. Наступним поколінням DLT стала Etherium – платформа для створення децентралізованих онлайн-сервісів на базі блокчейна, які працюють на базі смарт контрактів, та відповідна криптовалюта [2]. За 15 років інтенсивного розвитку систем, заснованих на DLT, та їх практичного застосування, виявилися як їхні переваги, так і властиві їм недоліки. На усунення цих недоліків спрямовано розробку та створення численних DLT платформ. У цьому аспекті тема даної роботи, присвяченої розробці та тестовим випробуванням швидкодіючої та високомасштабованої децентралізованої системи обробки транзакцій є досить актуальною.

Аналіз існуючих технологій побудови розподілених реєстрів. DLT, що засновані як на класичному блокчейні, так і на платформах Etherium, широко використовуються в різних практичних додатках [3]: фінансових послугах, включаючи платіжні системи [4,5], медицині та охороні здоров'я [6,7] , секторі нерухомості [8], підтримці Інтернету речей (IoT) [9,10], управлінні логістикою [11], енергетиці [12,13], послугах, що засвідчують особу (ID) [14] та ін. В процесі широкого впровадження DLT гостро проявилася передбачена раніше Бутеріним трилема блокчейна [15]. Трилема блокчейна є концепцією, яка описує три основні аспекти блокчейн-технології: децентралізацію, масштабованість та безпеку. Ця концепція стверджує, що неможливо одночасно досягти повної децентралізації, високої масштабованості та безпеки в блокчейні . Компоненти трилеми розуміються таким чином.

1. Децентралізація. Будь-яка DLT спрямована на децентралізацію, тобто рівномірний розподіл контролю та участі між вузлами мережі. Це гарантує стійкість мережі та підвищує довіру учасників. Однак повна децентралізація може призвести до низької пропускної здатності мережі та тривалого підтвердження транзакцій.
2. Масштабованість. Масштабованість відноситься до здатності децентралізованого реєстру обробляти велику кількість транзакцій і підтримувати мережу, що росте. Висока масштабованість дозволяє швидко та ефективно обробляти транзакції. Однак реалізація високої масштабованості може призвести до зменшення децентралізації та вразливості безпеки. Розподілена система повинна мати механізм масштабування для адаптації до зміни робочого навантаження у дуже широких межах. Однак, наприклад, швидкість обробки даних у відомих популярних системах Bitcoin та Etherium невисока – ці системи обробляють приблизно 7 та 20 транзакцій за секунду (tps) відповідно. Ці показники незрівнянні з традиційними централізованими системами, що обробляють тисячі транзакцій за секунду [16].
3. Безпека. Блокчейн забезпечує безпеку шляхом використання відповідних елементів криптографії та згоди більшості учасників мережі. Високий рівень безпеки в блокчейні вимагає високої обчислювальної потужності та достатньої кількості вузлів у мережі для підтвердження та підтримки надійності транзакцій. Однак підвищення безпеки може призвести до збільшення часу та ресурсів, необхідних для обробки транзакцій. Трилема блокчейна вказує на необхідність балансування цих трьох аспектів та вибору пріоритетів у розробці та реалізації блокчейн-рішень. Компроміс між децентралізацією, масштабованістю та безпекою є ключовим фактором при проектуванні та впровадженні блокчейн-систем. Таким чином, існує гостра необхідність у розробці та створенні високомасштабованої розподіленої системи з високою швидкістю обробки транзакцій.

Мета роботи. Мета роботи – розробка платформи децентралізованого реєстру з покращеними характеристиками масштабованості та швидкості обробки транзакцій.

Основна частина. Наступним поколінням технології побудови розподілених реєстрів слід вважати подання послідовності транзакцій як спрямованого ациклічного графа
(directed acyclic graph , DAG) [18]. Технологія на основі DAG побудована на поданні всієї множини транзакцій у вигляді направленого графа. Вершинами графа є транзакції (архітектура TxDAG) або блоки транзакцій (архітектура BlokDAG). Ребра графа з'єднують кожну вершину з усіма раніше утвореними (батьківськими) блоками, які ще не мають посилань. Таким чином, вся множина транзакцій представляється у вигляді спрямованого дерева. Далі вирішується відома в теорії графів задача лінійного топологічного впорядкування графа [19]. У результаті

дерево транзакцій перетворюється на лінійно впорядковану послідовність блоків з однаковим напрямом ребер – від останніх за часом утворення до раніше утворених. Це створює можливість застосування правила консенсусу для підтвердження і верифікації блоків. Архітектура BlokDAG була обрана як основна для побудови системи розподіленого реєстру з підвищеною швидкістю обробки транзакцій при високій масштабованості. Ці переваги BlokDAG у порівнянні з традиційним блокчейном досягаються за рахунок асинхронності утворення нових блоків у BlokDAG. Блокчейн побудовано на очікувані утворення нового блоку після верифікації попереднього елементу ланцюжка. У BlokDAG блоки утворюються незалежно від верифікації попередніх, а власне ланцюжок формується внаслідок топологічного впорядкування. Крім того, BlokDAG архітектура має парадоксальну, на перший погляд, але доведену властивість [18] – зі збільшенням числа користувачів системи швидкість обробки блоків / транзакцій зменшується.

Для подальшого прискорення обробки транзакцій запропоновано двошарову модель побудови системи. Основна мережа, призначена для формування та розповсюдження блоків, виконана за технологією BlokDAG (шар 1). Операції, пов'язані з верифікацією блоків на підставі протоколу консенсусу, винесені до координаційної мережі, що працює за технологією традиційного консенсусу (шар 2).

Як і в системі Etherium [2] для обробки транзакцій застосована дискретна часова шкала. Мінімальним інтервалом часу є слот тривалістю 4 с протягом якого дії шарів синхронізуються. Користувачі повинні створити та розподілити по мережі свій блок під час слота. Слоти поєднуються в епохи. Епохи призначені для підбиття проміжних результатів мережі. У запропонованій моделі епоха складається із 32 слотів.

Основним технологічним структурним елементом мережі є вузол (node, нода). Вузлом є зареєстрований сервер в мережі, що зберігає всі відповідні записи у вигляді реєстру. На кожному вузлі може бути розгорнуто певну кількість логічних структурних елементів, які умовно називатимемо Workers (Працівники), їх облікові записи мають необхідні дані для участі у протоколі консенсусу PoS [20]. Кожен Worker після включення до системи складається з двох компонентів з незалежними адресами – Утворювач блоків (Creator) та Координатор (Coordinator) (рис.1).

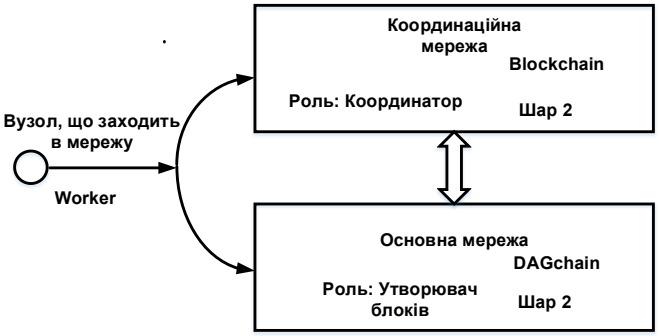

Рис. 1. Двошарова модель системи розподіленого реєстру

Функції обробки транзакцій розподілені між шарами системи в певний спосіб.

В основній мережі виконуються такі основні операції.

1. Пошук інших вузлів та підключення до них.
2. Прийом транзакцій від користувачів, розміщення в пул транзакцій та пересилання транзакцій далі по мережі.

3. Визначення на підставі методу перемішування, хто із творців створює блок у кожному слоті.
4. Вилучення транзакцій з пулу, додавання в блок, відправлення даного блоку іншим учасникам мережі.
5. Передача своєму координуючому вузлу порядку блоків, що входять в цей вузол.
6. Отримання від свого координуючого вузла порядку блоків для фіналізації. Під фіналізацією (або остаточністю) розуміється процес, після завершення якого транзакція в мережі може вважатися остаточною і не існує ризику фальсифікації (зміни) транзакції або блоку в упорядкованому ланцюжку.
7. Збереження історії блоків та транзакцій у вузлах реєстру.
8.Участь у синхронізації блоків та транзакцій.

Основні операції, які виконуються в координаційній мережі такі.

1. Визначення в кожному слоті епохи складу комітетів Proof of Stake та ролей координаторів у них (творець, атестатор, агрегатор).
2. Прийом результатів атестації від інших вузлів та передача її далі через мережу.
3. Додавання утворювачем в блок атестацій, раніше не доданих в блок.
4. Об'єднання сформованих агрегаторами атестацій в один мультипідпис .
5. Відповідно до отриманих атестацій та алгоритму консенсусу формування ланцюжка блоків, що підлягають фіналізації ; відправка фінального ланцюжка блоків у свій вузол основної мережі для фіналізації.
6. Синхронізація результату консенсусу з основною мережею.
7. Зберігання історії блоків та атестацій.
8. Зберігання стану координаторів (баланси, статус) у загальному стані мережі.

На підставі викладених архітектурних та алгоритмічних рішень розроблено платформу розподіленого реєстру Waterfall [21].

Основні властивості системи.

Мова програмування – Golang .

Архітектура – двошарова, основна мережа – BlockDAG , координаційна мережа – Blockchain .

Протокол консенсусу – удосконалений Proof of Stake.

Функціональність, що забезпечується, – обслуговування транзакцій з відомими і вбудованими токенами (включаючи NFT), обслуговування смарт-контрактів, розробка розподілених додатків dApps .

На рис. 2 наведено одну з екранних форм платформи Waterfall.

Рис.2. Екран виведення результуючого лінійного топологічного впорядкування BlockDAG.

Проведено навантажувальні експерименти для розробленої системи. Тестова мережа була сформована на базі серверів Amazon Elastic Compute Cloud. Тестова мережа працювала на 64 екземплярах t3.small (два ядра ЦП та 2 ГБ пам'яті) Amazon EC2. У ході експериментів було згенеровано пул приблизно зі 100 000 транзакцій та зафіксовано час, за який остання з них буде записана до реєстру. Були зроблені виміри масштабованості, Середня швидкість становила 2234 tps. Модифікована версія Waterfall обробила понад 3600 транзакцій за секунду при завантаженні ЦП менше 20%. На рис.3 наведено один із екранів з результатами тестування.

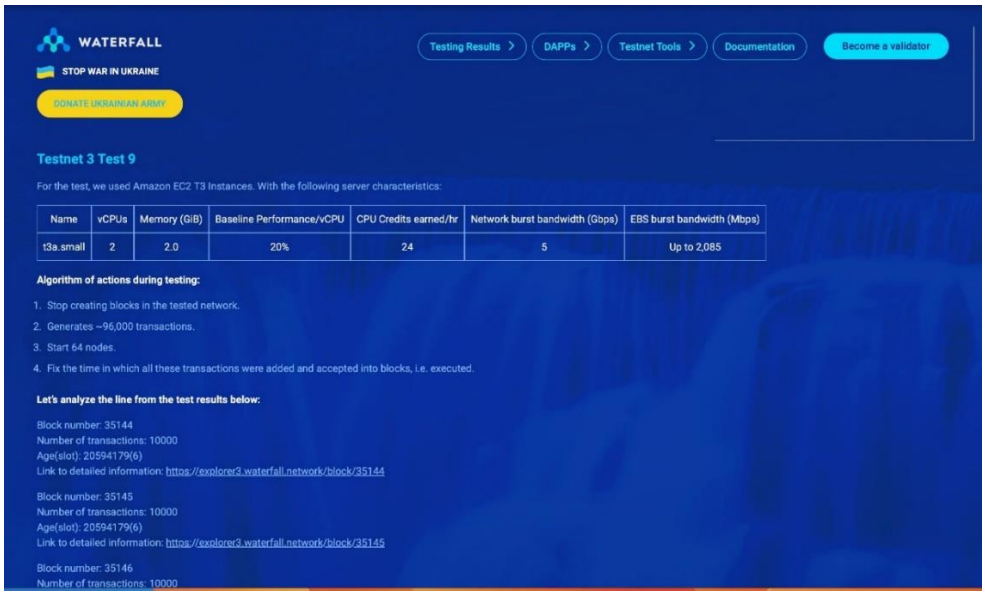

Рис.3. Приклад екрану з результатами тестування навантаження.

Поточна реалізація Waterfall використовує технологію Etherium EVM, що полегшує використання смарт-контрактів. Смарт-контракти для Ethereum можна копіювати і вставляти, при цьому вони успішно працюють у тестовій мережі Waterfall. Експерименти показали, що для імпорту більшої кількості децентралізованих додатків може знадобитися незначна зміна їхнього коду.

Безпека реалізації системи підтримується тими самими криптографічними протоколами, які добре зарекомендували себе у мережі Ethereum.

Хеш-функції – основна мережа – Keccak-256/SHA3, координаційна мережа – SHA256.

Цифрові підписи для формування ключів – вузли основної мережі – ECDSA (Elliptic Curve Digital Signature Algorithm) secp256k1, вузли координаційної мережі - підпис BLS (Boneh-Lynn-Shacham). Встановлено рекомендовану конфігурацію для успішного запуску вузла:

– Число ЦП – 2;
– Оперативна пам'ять – 4 Гб;
– SSD – 80 Гб;
– Інтернет трафік – 400 Гб/міс.

Результат та обговорення. Розроблена платформа Waterfall успадковує та покращує Ethereum 2.0. Крім того, платформа має ряд переваг:

1. Висока продуктивність – масштабовані в системі блокові структури на основі DAG дозволяють одночасно публікувати кілька блоків. Це формує DAG та забезпечує завершеність всіх транзакцій за умови, що блоки не конфліктують один з одним. Тому Waterfall може одночасно обробляти карти Visa, MasterCard та

Union.Pay на децентралізованому рівні навіть у години пік. Згідно з останніми проміжними лабораторними тестами, система могла обробляти 3600 транзакцій в секунду. Для порівняння зазначимо, що Visa обробляє близько 1700 транзакцій на секунду.

2. Низькі комісії за транзакції – архітектура спроектована таким чином, щоб підтримувати мінімальні комісії у різних сценаріях. Протокол динамічно масштабується зі зростанням навантаження на мережу. У той час, як продуктивність всієї системи збільшується, в тому самому слоті одночасно публікується більше блоків, а транзакційні збори знижуються в міру масштабування системи. Це знижує кількість операцій у пулі транзакцій навіть у години пік.

3. Низький фінансовий поріг входу – вузол із 6 Worker'ів коштує приблизно 1 920 доларів США.

4. Платформа обслуговує вбудовані токени – випуск та обслуговування токенів (включно з NFT) не потребують спеціальних смарт-контрактів, а виконуються за допомогою звичайних транзакцій, що значно знижує накладні витрати. Крім того, це робить їх використання більш доступним для широкого кола користувачів.

5. Динамічна настройка – платформа має механізми динамічної адаптації параметрів системи залежно від ситуації, що змінюється, зокрема, час слота, оптимальна кількість Worker'ів та деякі інші параметри налаштовуються автоматично.

Таким чином, платформа Waterfall забезпечує сприятливе середовище для надання та споживання широкого спектру послуг для ведення бізнесу та соціальної діяльності у зручному форматі загальнодоступного децентралізованого реєстру.

Висновки. Розроблено експериментальну платформу Waterfall, на основі технології децентралізованого реєстру з покращеними характеристиками масштабованості та швидкості обробки транзакцій. В основі платформи лежить запропонована автором двошарова модель розподіленого реєстру, що поєднує в собі основну мережу, побудовану за технологією DAGChain , та координаційну мережу, засновану на традиційній блокчейн -технології.

Платформа призначена для обслуговування транзакцій з різними токенами, включаючи NFT, обслуговування смарт-контрактів і розробки розподілених додатків. Тестування системи показало, що вона може обробляти в середньому 2234 транзакції за секунду при досить високому рівні масштабованості.

Список літератури

1. Maull R., Godsiff P., Mulligan C., Brown A., Kewell B. Distributed ledger technology: Applications and implications. *Strategic Change* . 2017. Vol. 26. No.5. P. 481-489. URL: https://doi.org/10.1002/jsc.2148.
2. Ethereum 2.0 Specifications. URL: https://bounties.gitcoin.co/grants/551/the-ethereum-20-annotated-specification
3. Jaoude J., Saade R. Blockchain Applications – Usage in Different Domains. *IEEE Access*. 2019. P. 45360-45381. https://doi.org/ 10.1109/ACCESS.2019.2902501.
4. Mohd J., Abid H., Ravi P.S, Rajiv S., Shahbaz K. Review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*. 2022. Vol.2. No.3. P.100073. https://doi.org/10.1016/j.tbench.2022.100073.
5. Mihus I. Evolution of practical use of blockchain technologies by companies. *Economics, Finance and Management Review*. 2022. No.1. P. 42–50. URL: https://doi.org/10.36690/2674-5208-2022-1-42 .
6. Abid H., Mohd J., Ravi P.S, Rajiv S., Shanay R. Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*. 2021. V.2. P.130-139. URL: https://doi.org/10.1016/j.ijin.2021.09.005.

7. Ghosh P.K, Chakraborty A., Hasan M., Rashid K., Siddique AH Blockchain Application в Healthcare Systems: A Review. *Systems* . 2023. V.11. P. 38. URL: https://doi.org/10.3390/systems11010038 .
8. Garcia-Teruel R. Legal challenges and opportunities of blockchain technology in the real estate sector. *Journal of Property, Planning and Environmental Law*. 2020. URL: https://doi.org/10.1108/JPPEL-07-2019-0039 .
9. Abbassi Y., Benlahmer H. IoT and Blockchain combined: for decentralized security. *Procedia Computer Science* . 2021. V. 191. P. 337-342. URL: https://doi.org/10.1016/j.procs.2021.07.045.
10. Patel C. IoT private preservation using blockchain IoT privacy preservation using blockchain. *Information Security Journal: Global Perspective* . 2021. No.31. URL: https://doi.org/10.1080/19393555.2021.1919795.
11. Perboli G., Musso S., Rosano M. Blockchain в Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases. *IEEE Access*. 2018. P.1-11. URL: https://doi.org/10.1109/ACCESS.2018.2875782.
12. Borkovcová A., Černá M., Sokolová M. Blockchain in Energy Sector – Systematic Review. *Sustainability*. 2021. V.22. No.14. P.14793. URL: https://doi.org/10.3390/su142214793.
13. Amanda A., Mika G., Masaru Y., Kenji T., Daishi S. Challenges and opportunities of blockchain energy applications: Challenges and opportunities of blockchain energy applications: Interrelatedness among technological, economic, social, environmental, and institutional dimensions. *Renewable i Sustainable Energy Reviews*. 2022. V. 166, P.112623. URL: https://doi.org/10.1016/j.rser.2022.112623
14. Sung C.S., Park J.Y. Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*. 2021.Vol. 34. No. 5. P. 1481-1505. URL: https:// doi.org/10.1108/JEIM-12-2020-0532
15. Buterin V. Proof Stake: Making of Ethereum i Philosophy of Blockchains. N.Y.: Seven Stories Press, 2022. 322 p.
16. Hafid A., Hafid A. S., Samih M. Scaling Blockchains: A Comprehensive Survey. *IEEE Access*. 2020. V.8. P.125244-125262. URL: https://doi: 10.1109/ACCESS.2020.3007251.
17. Qin W., Jiangshan Y., Shiping C., Yang X. SoK: Diving into DAG-based Blockchain Systems. 2022. 38p. URL: https://arxiv.org/pdf/2012.06128.pdf
18. Zverovich V. Modern Applications of Graph Theory. Oxford: Oxford University Press, 2021. 416p.
19. Chen T. Understanding Ethereum via Graph Analysis. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, Honolulu, HI, USA. 2018. P. 1484–1492. URL: doi: 10.1109/INFOCOM.2018.8486401.
20. Waterfall - DAG-based scalable smart-contract platform. URL: https://www.waterfall.network/

DEVELOPMENT OF A DECENTRALIZED LEDGER PLATFORM WITH IMPROVED CHARACTERISTICS

S.S. Grybniak

National Odesa Polytechnic University,
1, Shevchenko Ave. Odesa, 65044, Ukraine; e-mail: ssgrybniak@op.edu.ua

Over the fifteen years of its existence, distributed ledger technologies have found wide application in the field of financial turnover, cryptocurrency applications, and secure document management systems. The most popular today are the blockchain systems of Bitcoin and Etherium. Despite of their advantages – the immutability of processed transactions, decentralization, transparency – they have a serious drawback: low transaction processing speed and limited scalability. In this regard, it is difficult for them to compete with decentralized financial platforms that have transaction processing speeds orders of magnitude higher. The purpose of this work is to develop a decentralized ledger platform with improved scalability and transaction processing speed. The system was built on an architecture based on a directed acyclic graph – BlockDAG. BlockDAG architecture compares favorably with Blockchain in asynchronous operation. The ordering of blocks in it is carried out by topological linear sorting of the directed graph. In addition, the processing speed in BlockDAG increases with the increase in the number of users. The platform is built on a two-layer scheme and consists of two networks – the main BlockDAG network and the coordination network built on the basis of Blockchain. In the main network, blocks are created and distributed over the network. The coordination network performs the functions of block certification and their finalization. Proof of Stake consensus protocol applied. The system is implemented as an experimental Waterfall platform. The platform is designed to serve transactions with various tokens, including NFT, to serve smart contracts and develop distributed applications. System testing showed a high transaction processing speed combined with the required scalability.

Keywords: distributed ledger technologies , two-layer network , BlockDAG , Waterfall platform