УДК 004.75

С. С. Грибняк

ДВОШАРОВА МОДЕЛЬ МАСШТАБУЄМОГО РОЗПОДІЛЕНОГО ДЕЦЕНТРАЛІЗОВАНОГО РЕЄСТРУ

Не зважаючи на широке використання технології розподілених децентралізованих реєстрів, зокрема в популярних платформах Bitcoin і Etherium, їм притаманні суттєві недоліки. Головним з них є невисока швидкість обробки транзакцій. Для його усунення в цій роботі запропоновано двошарову модель розподіленого децентралізованого реєстру, що дозволить не тільки підвищити швидкість обробки транзакцій, а й збільшити масштабованість. Кожен з шарів моделі відрізняється як за функціями, що виконуються, так і за принципом створення мережі. Перший – є мережа, що побудована на архітектурі з використанням спрямованого ациклічного графу – DSGChain, яка саме створює блоки. Другим – є мережа, що являє собою класичний блокчейн. В цій мережі відбувається формування консенсусу Proof of Stake для валідації та фіналізації блоків. В рамках запропонованої моделі розроблено метод упорядкування блоків DAG. Метод базується на введеному понятті скелетних блоків. Метод дає змогу суттєво зменшити трафік між двома мережами. Розроблено метод формування оптимістичного (імовірнісного) консенсусу. Ймовірнісний консенсус дає змогу значно скоротити час фіналізації блоків. При формуванні комітетів для PoS консенсусу запропоновано використовувати новий метод перемішування на основі перетворення Tent, який суттєво підвищує рівень безпеки реєстру в цілому. На основі запропонованої моделі створено її програмну реалізацію у вигляді платформи Waterfall. Навантажувальні експерименти з тестовою мережею продемонстрували, що вона забезпечує швидкість обробки транзакцій більше 2000 tps при високому рівні масштабування. Таким чином, поєднання технологій блокчейн та DAGChain в одній моделі розподіленого реєстру дає змогу підвищити швидкість обробки транзакцій на порядки. Подальшим напрямком прискорення обробки даних є застосування шардингу в DAGChain мережі, що може ще більше підвищити показники ефективності розподіленого реєстру.

Ключові слова: *розподілений децентралізований реєстр, DAGChain, скелетний блок, ймовірнісний PoS консенсус.*

Вступ

Технології розподілених реєстрів (Distributed Ledger Technology, DLT) є сьогодні однією з найбільш революційних технологій у розробці розподілених систем обробки даних. Першим і класичним окремим випадком DLT стала технологія блокчейн і розроблена на її основі криптовалюта біткойн. За останнє десятиліття коло застосування блокчейнів та інших DLT швидко розширюється. Це викликає певні проблеми, пов'язані зі швидкодією роботи та масштабованістю розподілених реєстрів, тобто збереженням необхідних характеристик при різкому збільшенні числа користувачів. У цьому аспекті проблематика статті, присвяченої побудові моделі розподіленого реєстру з підвищеною швидкістю обробки даних та високою масштабованістю, є достатньо актуальною.

Актуальність

DLT стають все більш популярними завдяки безпечним та прозорим транзакціям та відсутністю посередників або центральних керуючих органів [1]. Очікується, що у зв'язку з зростанням попиту на цифрові послуги децентралізовані технології продовжуватимуть набирати популярності в найближчі роки. Технологія блокчейн може використовуватись практично у всіх сферах діяльності. Сюди належать насамперед різні фінансові послуги та платіжні системи [2, 3], медицина [4, 5], підтримка Інтернету речей (IoT) [6, 7] та багато інших галузей. Розподілена система повинна мати механізм масштабування для адаптації до зміни

робочого навантаження у дуже широких межах [8, 9]. Однак, наприклад, швидкість обробки даних у відомих популярних системах Bitcoin та Etherium невисока – ці системи обробляють приблизно 7 та 15 транзакцій за секунду (tps) відповідно. Ці показники незрівнянні з традиційними централізованими системами, що обробляють тисячі транзакцій на секунду [10]. Виникає проблема підвищення продуктивності обробки даних. Для її вирішення існує кілька варіантів, одним з яких є збільшення розміру блоку (кількість транзакцій у ньому), що призводить до проблеми, пов'язаної з розмірами блоку, а саме – блоки більшого розміру можуть помітно повільніше поширюватись по мережі [11]. Інший підхід пов'язаний із зменшенням тривалості слота – часу, що відводиться на створення блоку. У цьому випадку не виключається ситуація, коли блок може не встигнути розповсюдитися по мережі за відведений для цього час – такі блоки зазвичай відхиляються [12]. Третім підходом до проблеми підвищення продуктивності є паралельне створення кількох блоків, які посилаються на кілька попередніх блоків, таким чином формуючи спрямований ациклічний граф (directed acyclic graph, далі DAG). На основі DAG будується прискорена DLT, що називається BlockDAG [13]. В рамках цієї роботи пропонується поєднання технологій BlockDAG та блокчейн, що в перспективі має призвести до підвищення швидкості обробки даних у розподіленому реєстрі та збільшити масштабованість. Це зрештою дозволить вирішити вище сформульовану проблему.

Мета

Мета статті – побудова двошарової моделі розподіленого реєстру з підвищеною масштабованістю та швидкістю обробки транзакцій.

Задачі

1. Створення двошарової моделі розподіленого реєстру на основі двох мереж з поділом функцій.
2. Розробка способу упорядкування блоків DAG з урахуванням концепції структурних блоків.
3. Удосконалення методу формування ймовірнісного консенсусу для запропонованої двошарової моделі.
4. Експериментальне підтвердження покращених характеристик запропонованої моделі.

Двошарова модель розподіленого реєстру

Для підвищення швидкості обробки даних у розподіленому реєстрі та збільшення його масштабованості запропоновано двошарову модель розподіленого реєстру, що поєднує технології BlockDAG і блокчейн та складається із двох мереж.

Основним технічним структурним елементом мережі є вузол (node, нода) – це сервер, зареєстрований у мережі, який зберігає всі відповідні записи у вигляді реєстру. На кожному вузлі може бути розгорнуто певну кількість логічних структурних елементів, які умовно називатимемо Workers (Виробниками блоків), їх облікові записи мають необхідні дані для участі в протоколі консенсусу PoS [14]. Кожен Worker складається з двох компонентів з незалежними адресами – Валідатор (Validator) і Координатор (Coordinator).

Для поділу функцій оптимізації роботи та зберігання запропонована модель розподіленого реєстру містить два шари: мережу DAGChain та координаційну мережу (рис. 1).

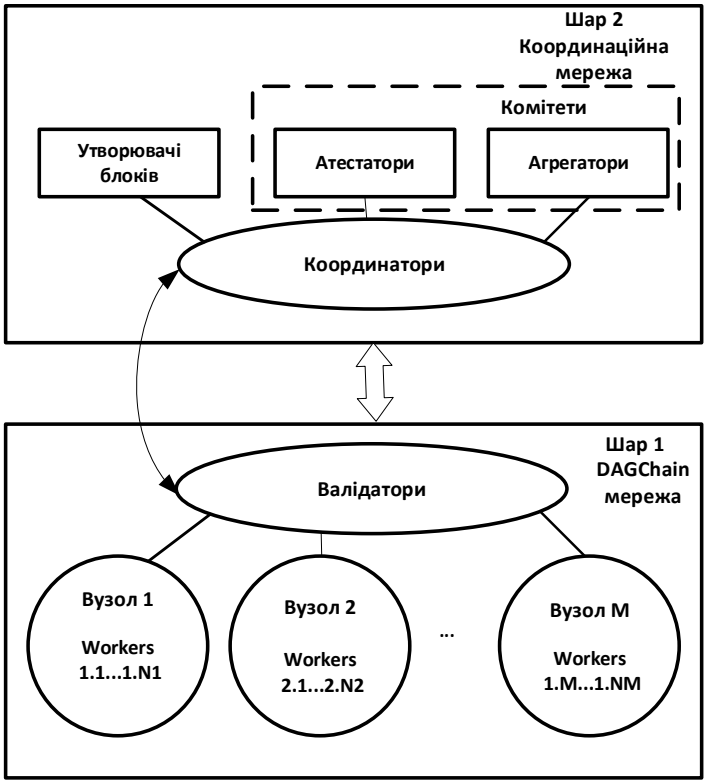

Рис. 1. Двошарова модель розподіленого реєстру

Мережа DAGChain будується на основі спрямованого ациклічного графу DAG, може приймати транзакції, об'єднувати їх у блоки та створювати еталонний DAG.

Координаційна мережа будується на основі блокчейна, відповідає за лінеаризацію DAG, фіналізацію блоків та вибір валідаторів, що створюють блоки у певному часовому інтервалі.

Ці дві мережі називатимемо шарами моделі (у деяких джерелах [14] застосовується термін рівні, levels).

Часова шкала в обох мережах розділена на часові інтервали – слоти тривалістю 4 с, протягом яких дії синхронізуються. Валідатори повинні створити та розподілити свій блок за час слота. Слоти поєднуються в епохи. Епохи призначені для підбиття проміжних результатів мережі. У запропонованій моделі епоха складається з 32 сотів. При цьому призначаються комітети Валідаторов для схвалення блоків на кожний наступний слот.

Функції DAGChain мережі та координаційної мережі принципово різні.

DAGChain мережа має наступні функції:

1. Пошук інших вузлів та підключення до них.

2. Прийом транзакцій від користувачів, розміщення в пул транзакцій та пересилання транзакції далі по мережі.

3. Визначення на підставі методу перемішування, хто з валідаторів створює блок у кожному слоті. Слід зазначити, що у запропонованій моделі застосований удосконалений метод перемішування, що дозволяє підвищити швидкість вибору відповідного валідатора та криптозахищеність системи [15].

4. Вилучення транзакцій з пулу, додавання їх у блок, відправлення цього блоку іншим учасникам мережі.

5. Валідація одержаних блоків.

6. Упорядкування блоків, визначення так званих скелетних блоків у кожному слоті.

7. Передача своєму координуючому вузлу порядку скелетних блоків, що входять до цього вузла.

8. Отримання від свого координуючого вузла порядку скелетних блоків для фіналізації. Під фіналізацією (або остаточністю) в DRT розуміється процес, після завершення якого транзакція в мережі може вважатися остаточною і не існує ризику фальсифікації (зміни) транзакції або блоку в упорядкованому ланцюжку.

9. Упорядкування транзакцій з використанням отриманих скелетних блоків від координуючого вузла та фіналізація блоків.

10. Збереження історії блоків та транзакцій у вузлах реєстру.

11. Участь у синхронізації блоків та транзакцій.

12. Обробка спеціальних транзакцій для активації / деактивації валідаторів, збереження поточного списку валідаторів, який використовується для визначення творців блоку в кожному слоті.

Координаційна мережа будується на основі блокчейна, в ній координатори можуть мати наступні ролі:

– творець блоку;

– атестатор, який підписує останній, на його думку, валідний блок у слоті;

– агрегатор, що поєднує результати атестації одним підписом.

Координуюча мережа має наступні функції:

1. Визначення квазівипадковим чином (за допомогою вдосконаленого алгоритму перемішування) у кожному слоті епохи складу комітетів та ролей координаторів у них (творець, атестатор , агрегатор).

2. Прийом результатів атестації від інших вузлів та передача її далі через мережу.

3. Додавання творцем блоку порядку скелетних блоків, який він отримав від свого вузла, а також додавання до блоку атестацій, які раніше не були додані до блоку.

4. Відправлення атестаторами свого підпису останнього блоку, в якому містяться скелетні блоки, з якими вони згодні. Цей блок у своєму минулому має перший блок минулої епохи з результатом фіналізації.

5. Об'єднання агрегаторами атестацій, в один підпис, щоб зменшити кількість повідомлень, що пересилаються між вузлами.

6. Відповідно до отриманих атестацій та алгоритму консенсусу формування ланцюжка скелетних блоків, що підлягають фіналізації.

7. Відправлення фінального ланцюжка скелетних блоків у свій вузол DAGChain мережі для фіналізації.

8. Синхронізація результату консенсусу з DAGChain мережею.

9. Отримання інформації з DAGChain мережі про початок активації/деактивації валідаторів, надсилання у відповідь інформації, коли валідатор буде активований/деактивований.

10. Нарахування нагород та штрафів координаторам на підставі отриманих атестацій.

11. Зберігання історії блоків та атестацій.

12. зберігання стану координаторів (баланси, статус) у загальному стані мережі.

Метод упорядкування блоків DAG

Для зменшення трафіку між DAGChain мережею та координаційною мережею в рамках цієї роботи запропоновано метод упорядкування блоків DAG з урахуванням концепції структурних блоків.

Визначимо поняття скелетних блоків та особливості їх застосування. У DAGChain кожен блок посилається (спрямованими ребрами) на всі попередні, раніше утворені (батьківські) блоки. Іноді всю множину батьківських блоків називають «минулим» (past) цього блоку. Висотою блоку називатимемо кількість всіх батьківських блоків, на які посилається цей блок.

Визначення. Скелетний блок – це блок слота, який задовольняє наступним правилам:

1) Має найбільшу висоту.

2) Якщо таких блоків декілька, то береться блок, який посилається на більшу кількість попередніх блоків.

3) Якщо таких блоків декілька, то береться той, у якого найменший хеш-код або який виділений після процедури перемішування.

Оскільки кожен блок зберігає дерево Меркла, фактично скелетний блок зберігає в «упакованому» вигляді все «минуле» блоків цього слота. Тому можна передавати до координаційної мережі не всі блоки слота, а лише скелетні блоки. Це дозволяє зменшити трафік між DAGChain мережею та координаційною мережею в n разів, де n – число блоків, утворених у слоті.

Це дозволило запропонувати метод упорядкування блоків DAG із застосуванням скелетних блоків, який реалізується наступним алгоритмом:

1. Визначається скелетний блок кожного нефіналізованого слота, скелетні блоки впорядковуються по порядку їхнього прямування від меншого номера слота до більшого.

2. Вибирається перший скелетний блок.

3. Беруться нефіналізовані батьківські блоки цього блоку та впорядковуються за висотою (за принципом «чим більше, тим раніше»); якщо висота однакова, то блоки впорядковуються за кількістю посилань на попередні блоки (батьківські); якщо кількість посилань однакова, то блоки впорядковуються за найменшим хеш-кодом або за допомогою процедури перемішування. Цей блок вставляється у список перед скелетним блоком.

4. Рекурсивно повторюється пункт 3 для вкладених батьківських блоків до тих пір, поки не прийдемо до того, що всі батьківські блоки або вже фіналізовані, або вже є в упорядкованому списку. Батьківські блоки вставляються до списку перед обраним блоком.

5. Повторюються пункти 3 – 4 з усіма скелетними блоками по порядку.

В результаті утворюється впорядкована послідовність всіх блоків DAG.

PoS консенсус у двошаровій моделі

Основне завдання, яке виконують учасники координаційної мережі (координатори) – це формування узгодженої спільної думки про стан мережі, яка згодом не змінюється, а лише доповнюється новими даними. Існує два підходи до формування консенсусу, вибір яких обумовлюється співвідношенням «ймовірність вірного рішення / час прийняття рішення (фіналізація рішення): повний (фінальний) PoS консенсус або оптимістичний (імовірнісний) консенсус.

У пропонованій моделі, як правило, використовується повний (фінальний) PoS консенсус для узгодження стану мережі, який працює за наступним алгоритмом:

1. За повного консенсусу кожен координатор протягом епохи голосує за перший валідний блок попередньої епохи.

2. Якщо блок набрав більше 2/3 голосів всіх координаторів, то блок вважається фіналізованим, та, як наслідок, ланцюжок скелетних блоків DAGchain мережі від минулого фіналізованого блоку теж вважається фіналізованим і відправляється в DAGchain мережу як остаточно затверджений.

3. Якщо в епосі 32 слоти, а слот триває 4 секунди, то транзакція пройде через 2*32*4=256 секунд = 4 хвилини 16 секунд.

Але для низки практичних застосувань, щоб зменшити час фіналізації, в цьому дослідженні запропоновано удосконалення методу PoS консенсусу шляхом формування оптимістичного (імовірнісного) консенсусу, який реалізується наступним чином:

1. Атестатори слота в попередньому слоті обмінюються скелетними блоками, які вони бачать у DAGchain. Автор координуючого блоку використовує цю інформацію, щоб вказати оптимальний ланцюжок скелетних блоків і підвищити шанси на те, що за нього проголосує більшість.

2. Атестатори голосують не тільки за перший блок попередньої епохи, але й за останній

блок координуючої мережі (в ідеальному варіанті за блок, створений у цьому ж слоті), в якому міститься ланцюжок скелетних блоків, які він бачить у своєму DAGchain вузлі та згоден з наявною послідовністю.

3. Якщо початкова частина ланцюжка скелетних блоків повторилася *m* раз і за ці блоки проголосували більше половини учасників відповідних слотів, то цей ланцюжок є кандидатом на фіналізацію і відправляється в DAGchain вузол на попередню фіналізацію.

4. Після фіналізації ланцюжка скелетних блоків у DAGchain мережі він записується в блок координуючої мережі, і ці скелетні блоки вже не пропонуються далі як кандидати.

Такий підхід дозволяє значно зменшити час фіналізація рішення при достатній ймовірність вірного рішення. Так проведено моделювання запропонованого методу формування консенсусу (спільно з методом перемішування) та встановлено, що одержане при фінальному консенсусі впорядкування не зміниться з ймовірністю, не меншою 0,9. Але прогноз можливої фіналізації може бути отриманий за 3*4=12 секунд. Подальшого прискорення можна досягти шляхом зменшення тривалості слоту.

Експериментальна перевірка показників якості розробленої моделі

На сьогодні основні елементи запропонованої моделі двошарового розподіленого реєстру, що масштабується, із застосуванням викладених вище методів обробки даних реалізовані мовою програмування Golang [16]. Тестова мережа побудована на базі серверів Amazon Elastic Compute Cloud. Проведено навантажувальні експерименти. Для лабораторних досліджень тестова мережа працювала на 64 екземплярах t3.small (з двоядерним ЦП та 2 ГБ пам'яті) Amazon EC2.

У ході експериментів було згенеровано пул з приблизно 100 000 транзакцій і зафіксовано час, за який останню з транзакцій буде записано до реєстру. Встановлено, значне підвищення швидкості обробки транзакцій, так тестова мережа продемонструвала середню швидкість 2234 tps.

Висновки та напрямки подальших досліджень

В результаті дослідження вирішено проблему підвищення масштабованості та швидкості обробки транзакцій шляхом виконання наступних завдань:

1. Запропоновано двошарову модель розподіленого реєстру, що поєднує в собі основну мережу, побудовану за технологією DAGChain, та координаційну мережу, засновану на традиційній блокчейн-технології. Завдання, які вирішуються мережами, розділені за функціональною ознакою.

2. Розроблено спосіб прискореного впорядкування блоків DAG з урахуванням концепції структурних блоків.

3. Удосконалено метод формування ймовірнісного PoS консенсусу у рамках запропонованої двошарової моделі.

4. Створено двошарову мережу, яка реалізує розподілений реєстр із середньою швидкістю обробки транзакцій, що перевищує 2000 tps при досить високому рівні масштабування. Це експериментально підтверджує покращення характеристик запропонованої моделі.

Таким чином, всі поставлені завдання вирішено, мету дослідження досягнуто. Як напрям подальших досліджень розглядається побудова DAGChain мережі з шардингом із застосуванням підмереж, що може далі підвищити показники якості розподіленого реєстру.

СПИСОК ЛІТЕРАТУРИ

1. Decentralized platforms: Goals, challenges, and solutions / S. Grybniak, Y. Leonchyk, R. Masalskyi [et al.] // IEEE 7th Forum on Research and Technologies for Society and Industry Innovation (RTSI). – 2022. – P. 62 – 67. DOI : 10.1109/RTSI55261.2022.9905225.

2. Trivedi S. Systematic Literature Review on Application of Blockchain Technology in E-Finance and Financial

Services / S. Trivedi, K. Mehta, R Sharma // Journal of Technology Management & Innovation. – 2021. – Vol. 16, № 3. – P. 89 – 102. DOI:10.4067/S0718-27242021000300089.

3. Mihus I. Evolution of practical use of blockchain technologies by companies / I. Mihus // Economics, Finance and Management Review. – 2022. – Vol. 1. – P. 42 – 50. DOI:10.36690/2674-5208-2022-1-42.

4. Applications of Blockchain in the Medical Field : Narrative Review / Y. Xie, J. Zhang, H. Wang [et al.] // J. Med. Internet Res. – 2021. – Vol. 23, № 10. – P. 286 – 294. DOI: 10.2196/28613.

5. Blockchain Technology Applications in Healthcare : An Overview / A. Haleem, M. Javaid, R. Pratap [et al.] // International Journal of Intelligent Networks. – 2021. – Vol. 2. – P. 130 – 139. DOI:10.1016/j.ijin.2021.09.005.

6. Moudoud H. Towards a Scalable and Trustworthy Blockchain : IoT Use Case / H. Moudoud, S. Cherkaoui, L. Khoukhi // IEEE International Conference on Communications, Montreal, QC, Canada. – 2021. – P. 1 – 6. DOI : 10.1109/ICC42927.2021.9500535.

7. Abbassi Y. IoT and Blockchain combined : for decentralized security / Y. Abbassi, H. Benlahmer // Procedia Computer Science. – 2021. – Vol. 191. – P. 337 – 342. https://doi.org/10.1016/j.procs.2021.07.045.

8. Solutions to Scalability of Blockchain : A Survey / Q. Zhou, H. Huang, Z. Zheng [et al.] // IEEE Access. – 2020. – Vol. 8. – P. 16440 – 16455. DOI: 10.1109/ACCESS.2020.2967218.

9. A Survey on the Scalability of Blockchain Systems / J. Xie, F. R. Yu, T. Huang [et al.] // IEEE Network. – 2019. – Vol. 33, № 5. – P. 166 – 173. DOI: 10.1109/MNET.001.1800290.

10. Hafid A. Scaling Blockchains: A Comprehensive Survey / A. Hafid, A. S. Hafid, M. Samih // IEEE Access. – 2020. – Vol. 8. – P. 125244 – 125262. DOI: 10.1109/ACCESS.2020.3007251.

11. Brilliantova V. Blockchain and the future of energy / V. Brilliantova, T. W. Thurner // Technology in Society. – 2019. – Vol. 57. – P. 38 – 45. DOI:10.1016/j.techsoc.2018.11.001.

12. Comparison of block expectation time for various consensus algorithms / D. S. Kaidalov, L. V. Kovalchuk, A. O. Nastenko [et al.] // Radio Electronics, Computer Science, Control. – 2019. – Vol. 4. – P. 159 – 171. DOI:10.15588/1607-3274-2018-4-15.

13. Swaroopa Reddy B. UL-blockDAG : Unsupervised Learning based Consensus Protocol for Blockchain / B. Swaroopa Reddy, G. V. V. Sharma // IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore. – 2020. – P. 1243 – 1248. DOI: 10.1109/ICDCS47774.2020.00159.

14. Understanding Ethereum via Graph Analysis / T. Chen, Y. Zhu, Z. Li [et al.] // IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, HI, USA. – 2018. – P. 1484 – 1492. DOI: 10.1109/INFOCOM.2018.8486401.

15. Grybniak S. Basic principles of mixing functions based on the simplest linear and nonlinear mappings / S. Grybniak, D. Dmytryshin // Proceedings of Odessa Polytechnic University. – 2022. – Issue 2 (66). – P. 100 – 109. DOI: 10.15276/opu.2.66.2022.12.

16. Waterfall [Електронний ресурс] / Access mode : https://waterfall.foundation/.

Стаття надійшла до редакції 15.05.2023.
Стаття пройшла рецензування 25.05.2023.

Грибняк Сергій Сергійович – аспірант кафедри прикладної математики та інформаційних технологій.
Національний університет «Одеська політехніка.