

ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА
Шаховської Наталії Богданівні,
доктора технічних наук, професора, завідувачки кафедри систем штучного
інтелекту Інституту комп'ютерних наук та інформаційних
технологій Національного університету «Львівська політехніка»
на дисертаційну роботу Грибняка Сергія Сергійовича
на тему
«Моделі та методи підвищення ефективності обробки транзакцій у
розподілених реєстрах»,
представлену на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки
галузь знань 12 – Інформаційні технології

1. Актуальність теми дисертації

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 Ethereum. 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. Тому дисертаційна робота, яку присвячено розв'язанню важливої науково-практичної задачі підвищення ефективності розподілених систем шляхом розробки моделей та методів обробки транзакцій у розподілених реєстрах для широкої низки практичних застосувань є своєчасною та актуальною.

Дисертаційна робота Грибняка Сергія Сергійовича виконана відповідно до планів наукової і науково-технічної діяльності Національного університету «Одеська політехніка», при виконанні проекту «Фундаментальні та поточні дослідження та розробки для Проекту Водоспад, технології розподілених обчислень з відкритим вихідним кодом», який фінансувався організацією Digital Clever Solutions Inc., США.

Структура та обсяг дисертації

Дисертація складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації складає 146 сторінку, в тому числі: 103 сторінок основного тексту, 39 рисунків і 3 таблиці, список використаних джерел з 115 найменувань і 4 додатків.

У вступі наведена загальна характеристика роботи, а саме: її актуальність, поставлені мета й задачі досліджень, представлені методи досліджень, вказані новизна і практичне значення отриманих результатів, сформульовані основні положення, що виносяться на захист, наведені відомості про апробацію, публікації та реалізацію результатів дослідження.

У першому розділі В першому розділі дисертаційної роботи проведено аналіз проблем створення та використання технології розподілених реєстрів, як комплексної інформаційної технології. Показано, що незважаючи на широку затребуваність та на чисельні дослідження та розробки в області технологій розподілених реєстрів, при впровадженні стикаються з проблемою недостатньою ефективністю існуючих рішень щодо швидкості обробки транзакцій при високих масштабуванні та криптозахищеності, усуненню якої і присвячене дане дослідження. Сформульовано мету та задачі дослідження.

У другому розділі запропоновано моделі та методи підвищення швидкості обробки транзакцій та масштабованості розподіленого реєстру, а саме:

- запропоновано двошарову модель розподіленого реєстру, яка поєднує основну мережу, побудовану за технологією BlockDAG, та координаційну мережу, що базується на традиційній блокчейн технології;
- модель скороченого обміну інформацією між DAGchain мережею та координаційною мережею на основі поняття скелетного блоку;
- метод прискореного PoS консенсусу в двошаровій моделі розподіленого реєстру на основі k -кратної перевірки повторення початкової частини ланцюжка скелетних блоків і голосування за ці блоки більше половини учасників відповідних слотів;

— методика визначення оптимального розміру комітету та розподілу Worker'ів залежно від їх загальної кількості в мережі та очікуваної помилкової частки.

У третьому розділі розроблено досліджено можливість застосування найпростіших положень теорії динамічних систем для захисту протоколу PoS від можливих маніпуляцій під час вирішення завдань псевдовипадкового вибору у координаційній мережі. Запропоновано метод перемішування даних за допомогою бієктивного відображення, яке є суперпозицією лінійного та найпростішого нелінійного відображення q-Tent, що дозволило здійснити процес якісного перемішування при формуванні PoS консенсусу, і тим самим захистити процес обробки транзакцій у розподілених реєстрах від можливих маніпуляцій.

У четвертому розділі розроблено експериментальну платформу Waterfall, що успадковує основні принципи Ethereum 2.0. Платформа Waterfall забезпечує сприятливе середовище для надання та споживання широкого спектру послуг для ведення бізнесу та соціальної діяльності у зручному форматі загальнодоступного децентралізованого реєстру. Показано суттєве підвищення ефективності, що свідчить про те, що поставлену мету дослідження виконано.

У загальних висновках викладено основні наукові та практичні результати виконаного дослідження, з якими можна погодитися.

У додатках представлено довідки впровадження.
Анотація дисертації стисло відображає її основні положення.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Наукові положення, висновки та рекомендації роботи достатньою мірою обґрунтовані, оскільки базуються на аналізі сучасних та загальновизнаних літературних джерел в таких галузях як аналіз даних, розподілені інформаційні системи, дискретна математика, експертне оцінювання та великій кількості експериментальних досліджень. Такий підхід підтверджує достовірність наукових положень, висновків та рекомендацій. Достовірність отриманих

теоретичних результатів підтверджується їх узгодженістю з результатами проведених експериментів для різних прикладних завдань.

Крім того, обґрунтованість наукових положень, висновків та рекомендацій підтверджується коректним застосуванням математичного апарату, даними комп'ютерних досліджень та практичними результатами, які підтверджуються наведеними у додатках дисертації довідками.

3. Практична значимість розроблених моделей та методів

підтверджується тим, що розроблені рішення були використані підвищення ефективності (часу обробки транзакцій, підвищення масштабованості та криптостійкості розподілених реєстрів) розподілених систем для широкої низки практичних застосувань.

Розроблено платформу Waterfall, що успадковує основні принципи Ethereum 2.0, але завдяки розробленим моделям та методам має більшу ефективність за низкою показників, що дозволяє її рекомендувати до широкого кола прикладних завдань, де використовуються розподілені реєстри.

Розроблені в роботі методи та інструментальні засоби отримали впровадження у діяльності Комунального підприємства «Теплопостачання міста Одеси» та знайшли відображення у навчальному процесі та науковій діяльності Національного університету «Одеська політехніка».

4. Новизна наукових положень, висновків та рекомендацій

В роботі визначено ряд нових наукових результатів, які є значущими для підвищення ефективності підвищення ефективності розподілених систем для широкої низки практичних застосувань:

- *вперше* розроблено двошарову модель розподіленого реєстру, що поєднує в собі основну мережу, побудовану за технологією BlockDAG, та координаційну мережу, що базується на традиційній блокчейн технології, що дозволило підвищити швидкість обробки транзакцій при суттєвому масштабуванні;
- *набула подальшого розвитку* модель скороченого обміну інформацією між DAGchain мережею та координаційною мережею на основі поняття скелетного

блоку, що дозволило скоротити обсяг трафіку між мережею BlockDAG та координаційною мережею і зменшити навантаження на систему загалом та підвищити швидкість обробки транзакцій;

- *вперше* розроблений метод прискореного PoS консенсусу в двошаровій моделі розподіленого реєстру на основі k -кратної перевірки повторення початкової частини ланцюжка скелетних блоків і голосування за ці блоки більше половини учасників відповідних слотів, що дозволило зменшити час отримання рішення до декількох секунд із ймовірністю, не меншою 0,9;

- *отримав подальший розвиток* метод перемішування даних за допомогою бієктивного відображення, яке є суперпозицією лінійного та найпростішого нелінійного відображення q -Tent, що дозволило здійснити процес якісного перемішування при формуванні PoS консенсусу.

5. Рекомендації щодо використання результатів дисертації

Розроблені в дисертаційній роботі моделі і методи доцільно використовувати для зменшення часу обробки транзакцій, підвищення масштабованості та криптостійкості розподілених реєстрів, що дозволило підвищити ефективність розподілених систем для широкої низки практичних застосувань.

Розроблену платформу Waterfall, що забезпечує сприятливе середовище для надання та споживання широкого спектру послуг для ведення бізнесу та соціальної діяльності у зручному форматі загальнодоступного децентралізованого реєстру, доцільно використовувати для обслуговування транзакцій з різними токенами, включаючи NFT, обслуговування смарт-контрактів і розробки розподілених додатків.

Запропоновані автором рішення доцільно використовувати в навчальних цілях при викладанні дисциплін пов'язаних розподіленими інформаційними системами, базами даних, захистом інформації.

6. Повнота викладу в наукових публікаціях, зарахованих за темою дисертації, відсутність порушення академічної доброчесності

Основні положення і практичні результати дисертаційної роботи доповідалися та одержали схвалення на таких конференціях: 7-й форум з IEEE досліджень і технологій для суспільства та промислових інновацій (Париж, Франція, 2022 рік), 1-й глобальний IEEE блокчейн-форум з нових технологій (м. Ірвін, США, 2022 рік), Міжнародна конференція IEEE з блокчейну, розумної охорони здоров'я та нових технологій (SmartBlock4Health) (м. Бухарест, Румунія, 2022 рік), Міжнародна конференція «Адаптивні технології управління навчанням ATL-2022» (Київ, 2022 рік).

Основні результати дисертаційної роботи викладено в 14 публікаціях, з них: 5 статей у наукових фахових виданнях України з технічних наук, 9 публікацій у зарубіжних наукових періодичних виданнях з напрямку, з якого підготовлено дисертацію, і працях і матеріалах наукових конференцій, 4 з яких проіндексовано наукометричною базою SCOPUS.

Таким чином, чинні вимоги до кількості публікацій виконано.

Публікація автором результатів досліджень у рецензованих виданнях, які передбачають попередню перевірку матеріалів на відсутність запозичень є одним із елементів підтвердження відсутності порушень академічної доброчесності. В цілому у дисертаційній роботі порушень академічної доброчесності не виявлено.

7. Зауваження згідно змісту та оформлення дисертаційної роботи

1. Перший розділ значно перевантажено довідковою інформацією, більшість з якої далі не застосовано.

2. На рис. 2.1. дисертації (стор.53) та в анотації (рис.1, стор.3) наведено двошарова модель системи розподіленого реєстру, але, на жаль, її складові описано не достатньо повно. Зокрема незрозуміло, де в розробці використано позначені на рисунку шардингові мережі, і чи використано їх в дослідженні взагалі.

3. Нечітко сформульовано результати застосування ймовірнісного консенсусу. Чи є ймовірнісний консенсус обов'язковим для використання, чи він може застосовуватися опціонально?

4. В розділі 3 відсутнє порівняння запропонованого методу перемішування з використанням псевдохаотичного перетворення qTent з іншими відомими методами.

5. Присутня в роботі англomовна термінологія і багато англomовних аббревіатур ускладнюють читання, слід було б паралельно ввести їх переклад українською.

6. У роботі мають місце окремі стилістичні та синтаксичні неточності і похибки.

Наведені зауваження не впливають суттєво на загальне позитивне враження від дисертаційної роботи та не знижують науковий рівень і практичну цінність дисертації.

8. Загальний висновок

В цілому вважаю, що дисертаційна робота Грибняка Сергія Сергійовича «Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах» є завершеною кваліфікаційною науковою роботою, яка має науково-практичне значення, тема і зміст якого відповідає спеціальності 122 «Комп'ютерні науки».

Вона містить не захищені раніше наукові положення і нові науково обґрунтовані результати в галузі розподілених інформаційних систем. Результати дисертації можуть бути рекомендовані до використання в організаціях і науково-дослідних установах, які розробляють розподілені інформаційні системи.

Дисертаційна робота «Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах» за своїм змістом відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету

Міністрів України від 12 січня 2022 р. № 44, а її автор Грибняк Сергій Сергійович заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю – 122 Комп'ютерні науки, галузь знань – 12 Інформаційні технології.

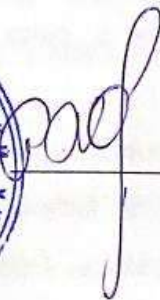
Офіційний опонент,
доктор технічних наук, професор,
завідувачка кафедри систем
штучного інтелекту Інституту
комп'ютерних наук та
інформаційних
технологій Національного
університету «Львівська
політехніка»

 Наталія ШАХОВСЬКА

Підпис засвідчую:

кандидат технічних наук, доцент,
вчений секретар Національного
університету «Львівська
політехніка»



 Роман БРИЛИНСЬКИЙ