ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора,
завідувача кафедри кібербезпеки
Західноукраїнського національного університету
Яцківа Василя Васильовича
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

Актуальність обраної теми.

Актуальність обраної теми зумовлена стрімким розвитком блокчейн-технологій та покращенням їх швидкості та масштабованості, що забезпечує конкурентоспроможність порівняно з централізованими фінансовими платформами. Технології розподілених реєстрів та побудовані на них системи, такі як Bitcoin та Ethereum, відзначаються великим впливом на різні галузі інформаційних технологій завдяки таким перевагам як децентралізація, прозорість та надійність. Але їх широкому впровадженню заважають все ще існуючи недоліки: низька швидкість обробки транзакцій (Блокчейн Bitcoin та Ethereum відомі своєю обмеженою пропускною спроможністю) та обмежена масштабованість.

Тому я вважаю, дисертаційна робота Грибняка Сергія Сергійовича, яка присвячена підвищенню ефективності розподілених шляхом розробки моделей та методів обробки транзакцій у розподілених реєстрах, є актуальною.

Оцінка обґрунтованості наукових положень, висновків і рекомендацій.

При вирішенні поставлених у дисертаційній роботі задач, створенні наукових положень, висновків та рекомендацій здобувачем застосовані дані, які

одержані з літературних джерел, а саме використана теорія розподілених систем та методи дискретної математики при розробці двошарової моделі розподіленого реєстру та моделі прискореного впорядкування блоків DAG; теорія прийняття рішень та експертного оцінювання при розробці методу формування ймовірнісного консенсусу; теорія чисел та теорія ймовірності при розробці методу квазівипадкового перемішування довільної числової множини; методи математичного та імітаційного моделювання при апробації запропонованих рішень. Вважаю, що створенні наукові положення, висновки та рекомендації можна вважати достатньо обґрунтованими.

Крім того, обґрунтованість наукових положень, висновків та рекомендацій підтверджується результатами моделювань, даними експериментальних досліджень та практичними результатами, які підтверджуються наведеними довідками практичних випробувань та результатами впровадження із позитивним ефектом.

Достовірність наукових положень, висновків і рекомендацій.

Достовірність наукових положень, висновків і рекомендацій, отриманих у дисертації, підтверджена результатами теоретичних та експериментальних досліджень, коректним застосуванням математичного апарату, сучасних методів наукового моделювання, а також впровадженням запропонованих рішень для обробки транзакцій, підвищення масштабованості та криптостійкості розподілених реєстрів, що дозволило підвищити ефективність розподілених систем для широкої низки практичних застосувань.

Наукова новизна положень, висновків і рекомендацій, сформульованих у дисертації.

Дисертаційна робота вирішує актуальну науково-практичну задачу підвищення ефективності розподілених систем шляхом розробки моделей та методів обробки транзакцій у розподілених реєстрах. Можна погодитись, що вона містить раніше незахищені наукові положення та отримані автором нові науково обґрунтовані результати. А саме:

– *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 тим самим 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 консенсус.

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 напряму, з якого підготовлено дисертацію, і працях і матеріалах наукових конференцій, 4 з яких проіндексовано наукометричною базою SCOPUS.

Таким чином, вимоги «Тимчасового порядку присудження ступеня доктора філософії», затвердженого КМУ № 167 від 06.03.2019 р. зі змінами, згідно постанови КМУ № 979 від 21.10.2020 р. та №609 від 09.06.2021 р. 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.

Аналіз змісту та форми дисертаційної роботи.

За своїм змістом дисертаційна робота здобувача Грибняка Сергія Сергійовича повністю відповідає Стандарту освітньо-наукової програми підготовки доктора філософії зі спеціальності 122 «Комп'ютерні науки», галузі знань 12 «Інформаційні технології» та напрямкам досліджень відповідно до третього (освітньо-наукового) рівня вищої освіти « Комп'ютерні науки».

Робота написана на достатньому мовно-стилістичному рівні.

У вступі показано актуальність та особливості застосування технології розподілених реєстрів на основі блокчейну, відзначена недостатня ефективність існуючих рішень та обґрунтовано необхідність підвищення ефективності обробки транзакцій в розподілених реєстрах, що передбачає поєднання високої швидкості обробки транзакцій, високої масштабованості системи та достатньої криптозахищеності від маніпуляцій та атак. Поставлені мета й задачі досліджень, представлені методи досліджень, вказані новизна і практичне значення отриманих результатів, наведені відомості про апробацію, публікації та реалізацію результатів дослідження.

У першому розділі проведено аналіз існуючих технологій DLT, встановлені їх переваги та недоліки. Показано, що розподілена система повинна

мати механізми обробки транзакцій та масштабування для адаптації до зміни навантаження у дуже широких межах.

Запропоновано шляхи підвищення ефективності обробки транзакцій та масштабованості розподіленого реєстру.

У другому розділі запропоновано досліджено шляхи підвищення ефективності обробки транзакцій та масштабованості розподіленого реєстру.

Для прискорення обробки транзакцій з високим рівнем масштабованості запропоновано двошарову модель системи, що поєднує в собі основну мережу, побудовану за технологією BlockDAG, та координаційну мережу, що базується на традиційній блокчейн технології.

Побудовано модель скороченого обміну інформацією між основною мережею та координаційною мережею, що зменшує інформаційне навантаження на систему в цілому та підвищує швидкість обробки транзакцій.

Розроблено метод прискореного PoS консенсусу в двошаровій моделі розподіленого реєстру.

У третьому розділі розроблено метод квазівипадкового перемішування довільної числової множини, що реально гарантує захищеність від подібних маніпуляцій. Розділ присвячений дослідженню можливості застосування у комп'ютерній криптографії найпростіших положень теорії нелінійних дискретних динамічних систем, основною характеристикою яких є хаотичність.

У четвертому розділі розроблено експериментальну децентралізовану платформу Waterfall, яка успадковує основні принципи Ethereum 2.0 та розвиває їх. Завдяки розробленим рішенням платформа Waterfall забезпечує низку переваг, порівняно з існуючими аналогічними технічними рішеннями. Проведені дослідження, що підтверджують одержані результати.

У висновках сформульовано основні результати дисертаційної роботи.

У додатках представлено довідки впровадження та додаткові матеріали.

Анотація дисертації коректно відображає її основні положення.

Зауваження до дисертаційної роботи.

В цілому дисертація і анотація до неї оформлені з дотриманням нормативних документів на оформлення результатів науково-дослідних робіт. Однак необхідно зауважити наступне:

1. Здобувач декларує як ефективність композицію швидкодії, масштабованості і крипто захищеності розподіленого реєстру. Але існує теорема Брюєра, яка зараз трансформувалася в відому трилемму блокчейну Бутеріна, яка проголошує, що збільшити одночасно всі три перелічені характеристики неможливо. Отже таке визначення ефективності не є цілком коректним.

2. Доцільно було більше уваги приділити взаємодії рівнів, зокрема, деталізувати, яка інформація передається між рівнями та привести структуру блоку.

3. В методиці застосування обміну інформації на основі хребетних блоків (2.2.2) сказано, що при інших рівних умовах блоки впорядковуються за найменшим хеш-кодом. Однак а роботі не розкрито поняття найменший хеш-код (ст.58).

4. В роботі не сказано, як вирішується проблема алгоритму PoS, така як тривалі періоди роз’єднання з мережею.

5. Незрозуміло, для чого ускладнювати систему, використовуючи на її різних шарах різні хеш-функції.

6. З якими розмірами блоку проведено тестові випробування розробленої здобувачем платформи? Очевидно розмір блоку має суттєво впливати на показники швидкодії обробки транзакцій, але інформація щодо цього питання в роботі відсутня.

7. В тексті розглянутої роботи присутні незначні стилістичні та граматичні огріхи.

Загальні висновки та оцінка дисертації.

Перелічені зауваження не є принциповими і такими, що піддають сумніву результати дослідження та ніяким чином не зменшують наукову і практичну цінність роботи та позитивне враження від впровадження її результатів.

Дисертаційна робота, яка представлена на відгук, є закінченою кваліфікаційною науковою працею, яка містить раніше не захищені наукові положення і одержані автором нові науково обґрунтовані результати в області підвищення ефективності обробки транзакцій в розподілених реєстрах.

В підсумку з оглядом на актуальність проблеми, вклад автора в теорію розподілених реєстрів, високий рівень виконаних досліджень та результати практичного впровадження вважаю, що дисертаційна робота «Моделі та методи підвищення ефективності обробки транзакцій у розподілених реєстрах» 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,
завідувач кафедри кібербезпеки
Західноукраїнського
національного університету _____ Василь ЯЦКІВ