

РЕЦЕНЗІЯ

на дисертаційну роботу

Колісніченка Вадима Юрійовича

на тему «Методи та програмні засоби аналізу блокчейн транзакцій»,
представлену на здобуття ступеня доктора філософії

в галузі знань 12 Інформаційні технології

за спеціальністю 121 Інженерія програмного забезпечення

Актуальність теми дисертації.

Актуальність теми дисертаційної роботи "Методи та програмні засоби аналізу блокчейн транзакцій" обумовлена швидким та всебічним розвитком блокчейн технологій, які стали основою для нових моделей бізнесу, фінансових інструментів та децентралізованих застосунків. В свою чергу стрімке зростання обсягу блокчейн транзакцій та різних блокчейн мереж створюють необхідність в нових методах та програмних засобах аналізу даних блокчейн транзакцій та ефективності мереж.

Запропоновані в дисертації методи спрямовані на вирішення ключових завдань аналізу блокчейн транзакцій, таких як асоціювання адрес з користувачами, аналіз потоків транзакцій та аналіз смарт-контрактів. Це дозволяє забезпечити прозорість, безпеку та ефективність функціонування блокчейн мереж, що є критично важливим для їх подальшого розвитку та інтеграції у різних галузях.

Розроблені методи можуть бути застосовані для моніторингу та аналізу транзакцій у реальному часі, що є надзвичайно важливим для оперативного виявлення та реагування на підозрілі активності. Дисертаційне дослідження робить внесок у розвиток інструментів для вивчення блокчейн-транзакцій, що є основою для подальшого розвитку методів децентралізованого аналізу даних.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. Покращено метод збору даних з блокчейн мереж, який використовує блокчейн-провідники для отримання даних про смарт-контракти, що дозволяє знизити ресурсоємність та підвищити ефективність аналізу.

2. Вдосконалено методологію аналізу OP_RETURN-скриптів у блокчейн мережі Bitcoin, що дозволяє автоматично класифікувати та аналізувати транзакції з використанням префіксних частин скриптів.

3. Вперше формалізовано протокол Peer Discovery для блокчейн мережі Rootstock шляхом детального аналізу вихідного коду вузла RSKj, що дозволяє створювати незалежні клієнти та оптимізувати роботу мережі.

4. Розроблено новий метод обходу вузлів блокчейн мережі, який забезпечує повний огляд структури мережі Rootstock та ефективно збирає дані про її вузли.

5. Запропоновано метод визначення відправника транзакцій у блокчейн мережі Rootstock, який враховує час отримання транзакцій та особливості мережі для ідентифікації вузлів-відправників.

6. Вперше розроблено комплексну архітектуру для аналізу блокчейн транзакцій, яка включає модульну структуру для інтеграції різних методів аналізу. Це дозволяє легко додавати нові компоненти та адаптувати систему до різних блокчейн мереж.

Достовірність та обґрунтованість наукових результатів забезпечується дослідженням ефективності розроблених методів та програмних засобів, а також підтвердженням результатів у експериментальних дослідженнях. Результати дисертації підтверджені публікаціями у наукових журналах та апробацією на підприємстві.

Наукові дослідження були виконані здобувачем на кафедрі інформатики та програмної інженерії КПІ ім. Ігоря Сікорського в рамках ініціативної теми «Хмарна платформа розроблення і управління функціонуванням критичних ІТ-інфраструктур» та відповідає напряму «Інформаційні та комунікаційні технології» з переліку пріоритетних напрямів науково-технічної діяльності.

Отже, в дисертаційній роботі поставлене наукове завдання підвищення ефективності програмних засобів аналізу блокчейн транзакцій виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Колісніченка В. Ю. повністю відповідає Стандарту вищої освіти зі спеціальності 121 Інженерія програмного забезпечення та напрямкам досліджень відповідно до освітньої програми Інженерія програмного забезпечення.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям інженерії програмного забезпечення.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Колісніченка Вадима Юрійовича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Виявлені збіги пов'язані з власними науковими працями

здобувача, які були раніше опубліковані для представлення основних результатів дисертації. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою, складається з вступу, чотирьох розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 144 сторінок.. Текст дисертації викладений логічно та послідовно, з використанням достатньої кількості сторонніх джерел та ресурсів, які належать до теми дослідження. Всі розділи містять відповідний матеріал.

У вступі розкрито актуальність теми дослідження в різних напрямках діяльності, наведено зв'язок роботи з науковими програмами, планами та темами, сформульовано мету і завдання дослідження, обґрунтовано об'єкт і предмет дослідження, визначено методи дослідження та наукову новизну одержаних результатів, а також наведено практичне значення отриманих результатів і структуру дисертації.

У першому розділі проведено огляд літератури та аналіз наявних методів і підходів до аналізу блокчейн транзакцій. Розглянуто області застосування аналізу у різних сферах. Виконано порівняльний аналіз сучасних систем аналізу блокчейн транзакцій, наведено огляд обмежень наявних методів. Виділено три основні групи задач, на які націлено аналіз транзакцій: асоціювання адреси з особою, аналіз великих потоків транзакцій та аналіз смарт-контрактів, а також сформульовано постановку завдань.

У другому розділі розроблено алгоритмічне забезпечення методів аналізу блокчейн транзакцій. Описано основні етапи розробленого методу застосування блокчейн-провідників для отримання даних з різних блокчейн-мереж. Описано методи виявлення вузлів блокчейн мережі Rootstock та визначення відправника транзакцій за допомогою псевдовузлів. Проаналізовано Peer Discovery і Wire протоколи та особливості OP_RETURN-скриптів у мережі Bitcoin.

У третьому розділі описано архітектуру комплексної системи аналізу блокчейн транзакцій, що підтримує різні типи блокчейн мереж. Розроблений прототип системи аналізу включає реалізацію розроблених методів, а також отримання даних, їх обробки та збереження. Описано програмне забезпечення для виявлення вузлів мережі Rootstock та визначення відправника транзакцій.

У четвертому розділі проведено експериментальну оцінку ефективності запропонованих методів та їх програмної реалізації. Перевірено ефективність методу застосування блокчейн-провідників для отримання даних з багатьох блокчейн-мереж. Оцінено ефективність методів виявлення та ідентифікації вузлів, а також визначення відправника транзакцій у блокчейн мережі Rootstock.

Проаналізовано ефективність методології аналізу OP_RETURN-скриптів у мережі Bitcoin.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи.

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких: 1 стаття у науковому виданні, включеному на дату опублікування до переліку наукових фахових видань України; 3 статті у періодичних наукових виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus, з яких 2 статей у виданнях, віднесених до першого — третього квартилів (Q1—Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports.

Публікації здобувача повністю відображають результати дисертаційного дослідження. Порухів принципів академічної доброчесності не виявлено. Крім наукового керівника, інших співавторів у публікаціях немає, що підтверджує беззаперечний особистий внесок здобувача.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. Зауваження до оформлення роботи:

- В тексті дисертації застосовано досить багато англіцизмів, які мають відповідники в українській мові.
- На рисунках 2.9 – 2.13 зображено процеси обміну даними між вузлами. Водночас не зрозуміло, в якій нотації виконані дані діаграми.

2. Зауваження до змісту роботи:

- автором приділено завищену увагу першому розділу дисертації, що робить зміст роботи незбалансованим;
- тема дисертації присвячена методам та програмним засобам аналізу блокчейн транзакцій. Водночас сама робота зосереджена на блокчейн-мережах Rootstock та Bitcoin. Включення аналізу інших мереж, таких як Ethereum, Tron, Polkadot або Solana додало б дослідженню більшої узагальненості та універсальності.

3. Використання ChatGPT в якості асистента для аналізу смарт контрактів може призводити до недетермінованих результатів, оскільки ChatGPT може видавати різні результати при одних і тих же запитах.

4. Робота зосереджена на аналізі блокчейн-транзакцій, в той же час не приділено уваги аналізу інформаційної безпеки. Так наприклад, аналіз

можливих вразливостей, загроз та методів їх нейтралізації в рамках розроблених методів дозволив би краще оцінити їх надійність та застосовність у реальних умовах.

5. Для порівняння ефективності розроблених методів обрано використання документо-орієнтованої розподіленої NoSQL бази даних MongoDB. В той же час саме для задач аналізу блокчейн транзакцій варто використати спеціалізовані графові бази даних, наприклад Neo4j, в яких вже реалізовано багато алгоритмів обходу графів як в глибину так і в ширину.
5. Дисертація не містить достатньо відомостей про можливості масштабування запропонованого рішення та його ефективність при обробці надвеликих масивів даних. Аналіз масштабованості допоміг би оцінити, наскільки розроблені методи здатні обробляти великі обсяги транзакцій у великих мережах та під великим навантаженням.
6. У розділі 2 представлені формальні представлення методів аналізу блокчейн транзакцій, однак дані представлення більше не використовуються в інших розділах. Зокрема, використання елементів математичного представлення дозволило б провести більш ґрунтовне дослідження ефективності розроблених методів.
7. У розділі 4 надано результати експериментів для різних блокчейн мереж, однак дані результати не містять порівняння з наявними методами, що дало б більш обґрунтовану оцінку результатів та запропонованих в дисертації підходів.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Колісніченка Вадима Юрійовича на тему «Методи та програмні засоби аналізу блокчейн транзакцій» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для галузі знань «12 Інформаційні технології». Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Колісніченко Вадим Юрійович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення.

Рецензент:

доцент кафедри інформатики та
програмної інженерії Національного
технічного університету України
“Київський політехнічний інститут
імені Ігоря Сікорського”,
кандидат технічних наук



/  /



« 8 » серпня 2024 року 