

ВІДГУК

офіційного опонента 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 даної теми зумовлена швидким зростанням популярності та застосування блокчейн технологій в різних сферах, що потребує постійного вдосконалення методів аналізу для забезпечення безпеки, ефективності та стійкості блокчейн мереж.

Аналіз блокчейн транзакцій є важливим аспектом для підтримки надійності та безпеки мережі, оскільки він дозволяє виявляти та усувати помилки у коді, оптимізувати продуктивність та масштабованість мережі, а також ідентифікувати потенційно неефективні місця у мережі. Це включає вивчення шаблонів трафіку, обробку запитів, аналіз затримок і пропускну здатності, що дозволяє виявляти вузькі місця та передбачати потенційні проблеми.

Виявлення вразливостей через аналіз блокчейн транзакцій є критичним для забезпечення безпеки мережі та дослідження минулих атак. Це охоплює відстеження підозрілих або нестандартних транзакцій, які можуть вказувати на спроби шахрайства, викрадення коштів, атаки типу "відмова в обслуговуванні" (DoS) або інші безпекові загрози. Таким чином, аналіз транзакцій стає ключовим інструментом у боротьбі з кіберзлочинністю та забезпеченні довіри до блокчейн технологій.

Розроблені методи можуть бути прямо або опосередковано застосовані як при аналізі транзакцій, так і для дослідження блокчейн мереж загалом. Це дозволяє підвищити ефективність програмних засобів аналізу блокчейн транзакцій, сприяючи розвитку більш надійних та безпечних блокчейн систем.

Зростання популярності криптовалют і технологій децентралізованих фінансів (DeFi) збільшує необхідність у більш складних методах аналізу транзакцій для запобігання шахрайству та відмиванню грошей. Ефективний аналіз блокчейн-транзакцій дозволяє виявляти підозрілі дії та забезпечувати безпеку користувачів

Робота є важливою як для наукових досліджень, так і для практичного застосування, зокрема в таких сферах, як розробка блокчейн систем, аудит

смарт-контрактів, розслідування злочинів, пов'язаних з блокчейн мережами, та трейдинг.

Дослідження, спрямовані на розробку нових методів та програмних засобів аналізу блокчейн-транзакцій, є надзвичайно важливими як з наукової, так і з практичної точки зору, забезпечуючи підвищення рівня безпеки, прозорості та ефективності блокчейн-мереж.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. Вперше розроблена архітектура програмного забезпечення для аналізу транзакцій у блокчейн-мережах, яка застосовує принцип інверсії керування, де окремі компоненти аналізу мережі самостійно ініціюють зв'язок та передають дані до ядра системи, що дозволяє легко інтегрувати нові мережі та методи аналізу.

2. Покращено метод отримання даних з блокчейн-мереж, який відрізняється від існуючих тим, що використовує блокчейн-провідники для отримання офчейн даних, що зберігаються провідником.

3. Вперше здійснено формалізацію протоколу Peer Discovery для блокчейн-мережі Rootstock шляхом аналізу вихідного коду вузла RSKj, що дозволяє реалізовувати незалежних клієнтів мережі та оптимізувати роботу цієї децентралізованої системи.

4. Розроблено метод обходу вузлів блокчейн-мереж, який дозволяє отримувати повну структуру мережі Rootstock, представляючи її у вигляді орієнтованого графа та послідовно опитуючи кожен нововиявлений вузол.

5. Вперше запропоновано метод визначення відправника транзакцій у блокчейн-мережі Rootstock, який аналізує час отримання нових транзакцій та враховує особливості мережі, що дозволяє точно ідентифікувати вузол, який першим транслиував транзакцію.

6. Вдосконалено методологію аналізу транзакцій у блокчейн-мережі Bitcoin, який дозволяє автоматично виділяти різні типи OP_RETURN-скриптів на основі частоти появи їх префіксних частин без попереднього знання форматів, що забезпечує розпізнавання та класифікацію збережених даних та протоколів.

Достовірність та обґрунтованість наукових результатів забезпечується тестуванням розроблених алгоритмів та інструментів, а також підтвердженням результатів експериментальними дослідженнями. Наукові результати дисертації підтверджені численними публікаціями у періодичних виданнях.

Отже, в дисертаційній роботі поставлене наукове завдання 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 співпадиння, можна зробити висновок, що дисертаційна робота Колісніченка Вадима Юрійовича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Наявні співпадиння є співпадиннями з власними науковими працями здобувача, опублікованими раніше для висвітлення основних результатів дисертації. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Таким чином, дисертаційна робота Колісніченка Вадима Юрійовича є оригінальною і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою. Викладення результатів є послідовним, доступним та зрозумілим, стиль мовлення відповідає науковим стандартам, використовуються загальноприйняті терміни відповідно до тематики дослідження.

Дисертація складається з вступу, 4 розділів, висновків, списку літератури та додатків. Загальний обсяг дисертації 144 сторінок.

У вступі обґрунтовано актуальність теми дослідження, сформульовано мету і завдання роботи, визначено об'єкт та предмет дослідження, описано методи дослідження, розкрито наукову новизну і практичне значення отриманих результатів.

У першому розділі проведено аналіз існуючих методів та засобів аналізу блокчейн-транзакцій, розглянуто області їх застосування в різних сферах, виділено основні групи задач, які вони вирішують. Проведено порівняльний аналіз сучасних систем аналізу блокчейн-транзакцій, включаючи блокчейн-провідники та комплексні платформи дослідження транзакцій.

У другому розділі розроблено алгоритмічне забезпечення для аналізу блокчейн-транзакцій, запропоновано чотири методи для здійснення аналізу транзакцій: метод застосування блокчейн-провідників для отримання даних з багатьох блокчейн-мереж, метод виявлення та ідентифікації блокчейн-вузлів, метод виявлення джерела транзакцій та метод аналізу OP_RETURN-скриптів.

Третій розділ присвячено розробці архітектури комплексної системи аналізу блокчейн-транзакцій, що підтримує різні типи блокчейн-мереж і дозволяє вбудовувати додаткові компоненти аналізу. Розглянуто процес розроблення прототипів запропонованих методів та їх інтеграцію до комплексної аналітичної платформи.

Четвертий розділ містить результати експериментального дослідження ефективності розроблених методів за допомогою реалізованих прототипів: метод застосування блокчейн-провідників для отримання даних з багатьох блокчейн-мереж, метод виявлення та ідентифікації блокчейн-вузлів, метод виявлення джерела транзакцій та метод аналізу OP_RETURN-скриптів.

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 демонструють високий науковий рівень, належну якість та відповідність принципам академічної доброчесності.

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

Недоліки та зауваження до дисертаційної роботи.

1. Дисертаційна робота фокусується на аналізі транзакцій у певних блокчейн-мережах, таких як Rootstock та Bitcoin. Включення результатів аналізу інших типів блокчейн-мереж могло б додати роботі більшої загальності та універсальності. Наприклад, дослідження ефективності запропонованих методів на мережах, що використовують різні консенсусні алгоритми або мають інші структурні особливості, могло б показати їхню адаптивність та ширший спектр застосування. Це розширило б можливості практичного застосування

розроблених методів у різних контекстах та забезпечило б краще розуміння їх потенціалу та обмежень.

2. У розділі 3 описано розробку багатопотокового прототипу системи збору даних одночасно з різних блокчейн-мереж, проте деякі аспекти практичної реалізації могли б бути висвітлені більш детально. Зокрема, інтеграція нових блокчейн-мереж та розширення функціоналу системи заслуговують на більш глибокий аналіз. Наприклад, можна було б детальніше розглянути процес додавання нових агентів для підтримки додаткових блокчейн-мереж, описати виклики, що виникають при цьому, та запропонувати шляхи їх вирішення. Це допомогло б краще зрозуміти масштабованість системи та її здатність адаптуватися до змін у блокчейн-екосистемі.

3. У розділі 4 представлено результати експериментального дослідження ефективності розроблених методів, проте варто було б надати більше інформації про критерії оцінки ефективності та результати експериментів. Більш детальний аналіз результатів експериментів дозволив би краще зрозуміти переваги та недоліки кожного методу, а також визначити оптимальні умови для їх застосування у різних контекстах. Це сприяло б більш обґрунтованому прийняттю рішень щодо використання цих методів у практиці.

4. У розділі 4.2 на сторінці 111 зазначено, що метод ідентифікації вузлів мережі Rootstock не може визначити реальні IP-адреси вузлів, які використовують VPN або TOR. Варто було б провести додаткові експерименти з метою оцінки впливу цих обмежень на точність ідентифікації вузлів та запропонувати можливі шляхи подолання таких обмежень. Це покращило б розуміння практичної ефективності запропонованого методу у реальних умовах.

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.

Офіційний опонент:

завідувач кафедри захисту інформації
Національного університету
«Львівська політехніка»,
доктор технічних наук, професор

/  /

Іван ОПІРСЬКИЙ

Підпис д.т.н., професора Опірського І. Р. засвідчую:

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





/ Роман БРИЛИНСЬКИЙ

“06” серпня 2024 р.