РЕЦЕНЗІЯ

на дисертаційну роботу

Горелікової Тетяни Олексіївни

на тему «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну», представлену на здобуття ступеня доктора філософії за спеціальністю 122 «Комп’ютерні науки»

Актуальність теми дисертації. У сучасних комп'ютерних науках та програмній інженерії проблема оптимізації децентралізованих обчислень та забезпечення надійності даних залишається одним із найгостріших питань. У сучасних умовах захист інформації виходить далеко за межі традиційного контролю доступу або шифрування даних. Особливої актуальності набувають питання протидії прихованій модифікації інформації, несанкціонованому видаленню даних та компрометації механізмів довіри в децентралізованих середовищах. Таким чином, актуальною є необхідність розробки нових математичних моделей для аналізу ймовірнісної поведінки систем блокчейн та рандомізованого підтвердження блоків. Практика експлуатації публічних блокчейн-мереж підтверджує гостроту цієї проблеми: відомі випадки успішних атак, унаслідок яких зловмисники отримували можливість переписати історію вже підтверджених транзакцій і завдати відчутних збитків. Показово, що такі інциденти відбувалися за умов використання стійких криптографічних примітивів, тобто джерелом вразливості виступали не алгоритми хешування чи цифрового підпису, а механізми консенсусу та передбачуваність процедур відбору вузлів-валідаторів. Це зміщує дослідницький фокус із власне криптографічного рівня на рівень організації процесів валідації, де випадковість і якість джерел ентропії набувають значення самостійного чинника безпеки. Додаткової ваги проблема набуває через розширення сфер застосування розподілених реєстрів – від державних реєстрів і фінансових платформ до медичних інформаційних систем. Отже, обраний напрям дослідження є актуальним і відповідає сучасним тенденціям розвитку комп'ютерних наук, системного аналізу та математичного моделювання інформаційних процесів.

Ступінь обґрунтованості мети і задач дослідження. Формулювання мети дисертаційного дослідження є чітким і концептуально завершеним: вона полягає у розробці та дослідженні методів захисту інформації від підміни та видалення з використанням технології блокчейн шляхом впровадження механізму рандомізованої валідації блоків і транзакцій, що забезпечує підвищення рівня цілісності даних, зниження ризиків компрометації та покращення ефективності функціонування системи. Декомпозиція загальної мети на окремі науково-прикладні завдання виконана з дотриманням системної логіки комп'ютерних наук, де кожне подальше завдання випливає з результатів розв'язання попереднього. Наявна структура забезпечує повний цикл розробки системи – від формалізації обчислювальних процесів і аналітичного оцінювання до алгоритмізації та створення програмних прототипів. Вона охоплює побудову формального апарату, аналітичне оцінювання стійкості, розробку стохастичних алгоритмів та їхню чисельну верифікацію шляхом програмного симуляційного моделювання. Коректно розмежовано об’єкт і предмет дослідження: об’єктом визначено процеси забезпечення цілісності та достовірності даних у розподілених блокчейн-системах в умовах децентралізованого функціонування, предметом – методи та механізми захисту інформації від підміни та видалення з використанням технології блокчейн. Така постановка задачі є цілком обґрунтованою та відповідає сучасним викликам побудови надійного програмного забезпечення.

Наукова новизна отриманих результатів. У процесі виконання дослідження автором запропоновано низку нових підходів до організації процедур перевірки та підтвердження інформації у блокчейн-мережах. Суттєвим науковим результатом є розвиток концепції випадкового вибору вузлів для здійснення процедур контролю коректності даних, що дозволяє підвищити стійкість системи до цілеспрямованих атак шляхом усунення передбачуваності механізмів валідації. Запропоновані рішення мають не лише прикладний, а й фундаментальний теоретичний характер. У роботі виконано формалізацію відповідних процесів, побудовано математичні моделі функціонування системи та проведено аналіз впливу основних параметрів на характеристики безпеки. Важливим результатом слід вважати дослідження ролі випадковості як самостійного фактора забезпечення

захищеності: автором показано, що якість ентропійного ресурсу безпосередньо впливає на ефективність процедур валідації. Значний науковий інтерес становлять результати використання фізичних джерел ентропії для формування випадкових послідовностей, що розширює уявлення про інтеграцію фізичних процесів у програмно-апаратні комплекси захисту. Не менш важливим є подальший розвиток методів забезпечення цілісності інформації у блокчейн-системах за рахунок рандомізованих механізмів перевірки та удосконалення підходів до формування криптографічно стійких випадкових послідовностей.

Практичне значення результатів. Практична цінність роботи полягає у готовності запропонованих рішень до алгоритмічної імплементації. Запропоновані методи можуть бути ефективно використані під час створення інформаційних систем, у яких критичне значення мають питання довіри до даних, їхньої незмінності та захищеності від зовнішніх втручань. До таких об'єктів належать державні реєстри, фінансові платформи, медичні інформаційні системи, корпоративні сховища даних та інші елементи критичної цифрової інфраструктури. Впровадження розроблених стохастичних алгоритмів дозволяє суттєво оптимізувати обчислювальне навантаження на вузли та зменшити обсяги комунікаційного трафіку в мережі. Варто відзначити якість проведених експериментальних досліджень: автором виконано серію обчислювальних експериментів; отримані результати характеризуються внутрішньою узгодженістю та добре корелюють із теоретичними положеннями роботи. Це свідчить про високий рівень достовірності сформульованих практичних рекомендацій для розробників програмного забезпечення.

Оцінка змісту дисертаційної роботи. Робота характеризується чіткою та логічною структурою викладу матеріалу, послідовністю аргументації та високим рівнем наукової культури в галузі комп'ютерних наук. У першому розділі дисертанткою виконано ґрунтовний за обсягом і глибиною аналіз сучасного стану наукових досліджень у галузі розподілених реєстрів та криптографічного захисту інформації: систематизовано підходи до забезпечення безпеки блокчейн-систем, досліджено особливості функціонування механізмів консенсусу, розглянуто переваги та обмеження відомих криптографічних методів, а також проаналізовано

фактори, які впливають на стійкість розподілених мереж до зовнішніх і внутрішніх загроз. У другому розділі розроблено теоретико-методологічну основу запропонованого підходу: метод випадкового вибору учасників і контрольних точок на основі криптографії еліптичних кривих, метод випадкового вибору вузлів-валідаторів із контролем цілісності за структурою Меркла та синтезований на їх основі метод рандомізованого підтвердження блоків, ефективність якого підтверджено серією обчислювальних експериментів. Третій розділ присвячено формуванню високоентропійного ресурсу як чинника криптографічної безпеки: обґрунтовано використання фізичних джерел випадковості, розроблено та експериментально перевірено прототип квантового генератора випадкових чисел на основі дробового шуму й оцінено вплив якості ентропії на ймовірність компрометації консенсусу. Автор демонструє вільне володіння сучасним методологічним апаратом комп'ютерних наук, теорією алгоритмів, мережевими протоколами та методами системного аналізу. Усі розділи дисертації підпорядковані єдиній архітектурній задумці, а викладені теоретичні положення підкріплені необхідними алгоритмічними схемами, таблицями та графічними залежностями результатів симуляції. Сформульовані висновки до розділів є обґрунтованими, стислими та логічно завершують відповідні етапи розробки системи. Текст роботи виконано науковою українською мовою з дотриманням усіх вимог щодо оформлення праць за спеціальністю 122 «Комп’ютерні науки».

Апробація та висвітлення результатів дисертаційної роботи. Основні положення та результати дисертаційної роботи Горелікової Т. О. доповідалися й обговорювалися на 7 наукових заходах, серед яких 4 міжнародні конференції та симпозіуми, 2 всеукраїнські наукові конференції і науковий семінар. За результатами дисертаційного дослідження опубліковано 11 наукових праць, серед яких 7 статей у наукових фахових виданнях України та 4 матеріали доповідей на наукових конференціях; 3 статті підготовлено одноосібно, 2 опубліковано англійською мовою. Опубліковані праці повністю відображають основний зміст дисертації, включаючи розроблені алгоритми, архітектурні схеми та результати програмного моделювання. Таким чином, ступінь висвітлення результатів роботи у науковій періодиці повністю відповідає вимогам МОН України.

Дискусійні питання та зауваження. При загальній високій оцінці теоретичної та практичної цінності дисертаційної роботи необхідно відзначити окремі дискусійні моменти та висловити деякі побажання щодо змісту й оформлення праці:

– у підрозділі 1.4 наведено експерименти, які спираються на відомі набори даних, однак конкретні набори не ідентифіковано – не наведено їх назв, авторів і посилань, які бажано було б навести для забезпечення відтворюваності результатів;

– у підрозділі 2.4 наведено опис тестової інфраструктури (Docker Swarm, мережі на 500, 1000 і 2000 вузлів, засоби моніторингу Prometheus і Grafana, лічильники PowerStat та Intel RAPL), проте не вказано апаратних характеристик вузлів і версій програмного забезпечення, які є суттєвими для повторення вимірювань часу підтвердження блоків та енергоспоживання;

– у роботі трапляються неузгодженість окремих позначень, подання частини формул без розшифровки величин, збої нумерації рисунків, етапів і посилань, а також поодинокі орфографічні та синтаксичні огріхи.

Вказані зауваження та висловлені побажання мають переважно методичний та структурно-оформлювальний характер. Вони ніяк не впливають на достовірність і обґрунтованість основних наукових результатів дисертації та не применшують її наукової новизни й практичної значущості.

Висновок. Дисертаційна робота Горелікової Тетяни Олексіївни «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну» подана на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп’ютерні науки» є цілісним, концептуально завершеним та самостійно виконаним науковим дослідженням. У роботі отримано нові, теоретично обґрунтовані та експериментально підтверджені наукові результати, які у своїй сукупності розв'язують важливе науково-прикладне завдання – підвищення рівня безпеки, цілісності та швидкодії децентралізованих систем шляхом розробки ймовірнісних моделей і рандомізованих алгоритмів підтвердження даних.

За актуальністю теми, рівнем наукової новизни, обґрунтованістю отриманих результатів, їх теоретичною та практичною значущістю дисертаційна робота відповідає вимогам «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 № 44 від 12 січня 2022 року, а також чинним вимогам до оформлення дисертацій.

Авторка дисертації, Горелікової Тетяни Олексіївни, заслуговує на присудження наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки».

Рецензент:
кандидат фізико-математичних наук,
доцент, завідувач кафедри програмної інженерії
Запорізького національного університету Андрій ЛІСНЯК