ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

Кандидата технічних наук, доцента Васильєвої Людмили Володимирівни на дисертаційну роботу Горелікової Тетяни Олексіївни «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну», подану на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки»

Оцінка актуальності вибору теми дослідження

Забезпечення цілісності, достовірності та незмінності інформації у розподілених інформаційних системах є одним із актуальних завдань сучасних комп'ютерних наук. Поширення децентралізованих цифрових платформ та застосування технології блокчейн у фінансових, державних, медичних, корпоративних інформаційних системах актуалізує необхідність удосконалення механізмів захисту даних від несанкціонованої модифікації, підміни та видалення. Особливого значення набуває стійкість механізмів консенсусу та валідації, оскільки їх компрометація може призвести до порушення довіри до всієї розподіленої системи.

Існуючі механізми консенсусу, поряд із перевагами децентралізованого зберігання та перевірки інформації, характеризуються низкою обмежень, пов'язаних із масштабованістю, обчислювальними витратами, концентрацією ресурсів та потенційною передбачуваністю процедур вибору учасників валідації. Цей аспект покладено в основу дисертаційного дослідження: авторкою висунуто та досліджено припущення щодо можливості підвищення стійкості блокчейн-систем шляхом рандомізації вибору вузлів-валідаторів та використання джерел випадковості з високим рівнем ентропії.

Актуальність роботи посилюється тим, що запропонований підхід розглядається не лише з позицій захищеності, а й з урахуванням продуктивності, масштабованості та обчислювальних витрат. Дисертанткою поставлено завдання експериментально оцінити механізм за показниками обчислювальних витрат, пропускної здатності, часу підтвердження транзакцій та мережевого навантаження, а також провести його порівняння з класичними механізмами консенсусу.

Таким чином, можна зробити висновок, що обрана тема дисертаційної роботи Горелікової Т. О. є актуальною, відповідає сучасним напрямам розвитку розподілених інформаційних систем, технологій блокчейн та методів забезпечення цілісності даних, а поставлене науково-прикладне завдання відповідає спеціальності 122 «Комп'ютерні науки».

Оцінка змісту і структури дисертаційної роботи

Робота складається зі вступу, трьох основних розділів, загальних висновків, списку використаних джерел і додатків.

У вступі обґрунтовано актуальність обраної теми, визначено мету, завдання, об'єкт і предмет дослідження, наведено використані методи, сформульовано положення наукової новизни та практичне значення результатів, подано відомості щодо апробації, публікацій та особистого внеску здобувачки. Об'єктом дослідження визначено процеси забезпечення цілісності та достовірності даних у розподілених блокчейн-системах, а предметом – методи та механізми захисту інформації від підміни та видалення з використанням технології блокчейн.

У першому розділі здійснено аналіз теоретико-прикладних засад захисту інформації із застосуванням технології блокчейн. Розглянуто архітектуру блокчейн-

систем, криптографічні механізми, особливості забезпечення надійності на рівні вузлів, систематизовано методи забезпечення надійності та проаналізовано актуальні загрози. За результатами проведеного аналізу обґрунтовано доцільність використання рандомізації як одного з чинників підвищення стійкості процесу валідації.

Другий розділ має переважно теоретико-модельний характер і присвячений моделюванню та обґрунтуванню алгоритму рандомізованої валідації блоків і транзакцій. Розроблено модель випадкового вибору вузлів-валідаторів, досліджено залежність імовірності компрометації від параметрів мережі та вибірки валідаторів, а також проведено імітаційне дослідження запропонованого підходу.

У третьому розділі розглянуто формування високоякісної випадковості та можливість застосування фізичного джерела ентропії. Розроблено прототип генератора на основі фотонного шуму, досліджено статистичні характеристики отриманих послідовностей та їхній вплив на механізм вибору валідаторів. Зокрема, авторкою порівнюються QRNG, CSPRNG та PRNG за показниками ентропії, автокореляції та рівномірності; наведені результати демонструють найкращі характеристики QRNG за використаними показниками.

Висновки по роботі узагальнюють основні отримані в дисертаційному дослідженні результати.

Загалом структура дисертації забезпечує послідовний перехід від аналізу предметної області до формалізації запропонованого підходу, його моделювання та експериментального дослідження.

Оцінка рівня обґрунтованості наукових положень дисертації, їх достовірність та новизна

Наукові положення, результати та висновки дисертації загалом є достатньо обґрунтованими. Для вирішення поставлених завдань використано методи теорії ймовірностей і математичної статистики, криптографії, теорії розподілених систем, математичного та імітаційного моделювання, теорії алгоритмів, системного аналізу та обчислювальної математики.

Важливою складовою обґрунтування результатів є поєднання теоретичного та чисельного дослідження. Імовірність компрометації оцінюється залежно від частки зловмисних вузлів, кількості валідаторів та характеристик випадкового вибору. Під час чисельного моделювання визначається частка раундів, у яких формується більшість зловмисних валідаторів, що використовується як чисельна оцінка ймовірності компрометації.

Досліджено також вплив кореляції випадкових послідовностей на ефективну кількість незалежних валідаторів і, відповідно, на ймовірність компрометації. Отримані результати показують, що збільшення кореляції між послідовними виборами погіршує характеристики безпеки, тоді як використання джерел із вищою якістю випадковості сприяє зменшенню відповідного ризику.

Достовірність результатів підтверджується узгодженістю теоретичних положень із результатами чисельного та імітаційного моделювання, проведеним статистичним аналізом випадкових послідовностей, а також апробацією результатів у наукових публікаціях і на конференціях.

Оцінка наукової новизни окремих результатів та дослідження в цілому

Наукова новизна дисертаційної роботи Горелікової Т. О. визначається розвитком підходів до забезпечення цілісності даних у блокчейн-системах на основі рандомізації

процесу валідації та дослідженням впливу характеристик джерела випадковості на стійкість механізму консенсусу.

Найбільш вагомим науковим результатом дисертації слід вважати запропонований механізм рандомізованої валідації блоків і транзакцій, у якому вибір підмножини вузлів-валідаторів здійснюється із застосуванням криптографічно та фізично захищених джерел випадковості. На відміну від детермінованого або потенційно передбачуваного формування складу валідаторів, запропонований підхід спрямований на зменшення можливості цілеспрямованого впливу на процес підтвердження транзакцій. Важливим є те, що цей результат у дисертації не обмежується описом алгоритмічної процедури, а досліджується шляхом математичного та імітаційного моделювання.

Науковий інтерес становить розроблена формальна модель випадкового вибору вузлів-валідаторів, у межах якої ймовірність компрометації визначається залежно від частки зловмисних вузлів та розміру вибірки валідаторів. Для вибірки без повернення використано гіпергеометричний розподіл, а для великих значень параметрів мережі розглянуто біноміальне наближення. Така формалізація забезпечує можливість кількісного дослідження стійкості запропонованого механізму та встановлення залежностей між параметрами системи і ризиком формування більшості зловмисних вузлів у складі валідаторів.

Окремою складовою наукової новизни є включення характеристик джерела випадковості до аналізу безпеки механізму валідації. У роботі досліджено зв'язок між статистичною залежністю послідовних виборів валідаторів та ймовірністю компрометації системи. Це дозволило авторці перейти від моделі, що враховує лише структурні параметри мережі, до моделі, в якій якість випадковості розглядається як один із факторів безпеки консенсусу.

Значущим результатом є також практичне дослідження можливості використання фізичного джерела ентропії на основі дробового шуму для реалізації механізму рандомізованої валідації. Авторкою створено апаратно-програмний прототип генератора, проведено статистичне дослідження сформованих ним послідовностей та виконано порівняльне дослідження QRNG, CSPRNG і PRNG з погляду їх впливу на характеристики процесу вибору валідаторів.

Позитивно слід оцінити комплексність верифікації запропонованого підходу. Дослідження включає математичне та імітаційне моделювання, лабораторні експерименти в контейнеризованому середовищі, статистичний аналіз результатів, дослідження масштабованості та продуктивності, а також аналіз характеристик створеного джерела ентропії.

Водночас при оцінюванні наукової новизни доцільно розмежовувати власне нові наукові результати та їх програмно-апаратну реалізацію. Самі по собі рандомізований вибір учасників консенсусу, застосування криптографічно стійких генераторів та використання фізичних джерел ентропії є відомими напрямами розвитку розподілених і криптографічних систем. Тому наукову новизну роботи коректніше пов'язувати насамперед із запропонованим авторкою комплексним механізмом рандомізованої валідації, його формалізацією, дослідженням залежності ймовірності компрометації від параметрів вибору валідаторів і характеристик випадковості, а також експериментальною перевіркою такого підходу.

З урахуванням зазначеного вважаю, що одержані в дисертації результати мають належний рівень наукової новизни для дисертаційного дослідження на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», а їх сукупність становить самостійний внесок у розвиток методів забезпечення цілісності даних у розподілених блокчейн-системах.

Практична цінність отриманих результатів

Практична цінність дисертаційного дослідження полягає у можливості використання запропонованих моделей і алгоритмів при проєктуванні та модернізації розподілених інформаційних систем на основі технології блокчейн.

Запропонований механізм може бути використаний для підвищення непередбачуваності процесу вибору валідаторів і зниження ризику формування скомпрометованої консенсусної групи. Практичний інтерес становить також розроблений підхід до використання фізичного джерела ентропії, статистичні властивості якого досліджено у роботі.

Авторкою показано потенційну можливість застосування результатів у фінансових, державних, медичних та корпоративних інформаційних системах, а також у розподілених системах штучного інтелекту, для яких принципове значення мають цілісність і достовірність даних.

Водночас практичне значення роботи доцільно трактувати насамперед як створення й експериментальне дослідження моделей, алгоритмічних і прототипних рішень. Перенесення запропонованих механізмів на промислові блокчейн-платформи потребуватиме додаткової перевірки в реальних розподілених середовищах.

Повнота відображення основних положень дисертації в опублікованих роботах

Основні результати дисертаційного дослідження відображено у 7 наукових статтях, а результати роботи також апробовано на всеукраїнських і міжнародних наукових заходах. У висновку про наукову новизну наведено відповідність публікацій конкретним підрозділам дисертації, що дозволяє простежити оприлюднення результатів усіх трьох основних розділів.

Тематика публікацій охоплює аналіз методів захисту інформації у блокчейн-системах, механізми захисту від підміни та видалення, рандомізоване підтвердження блоків, використання блокчейну для захисту медичних даних, а також розроблення джерела високої ентропії на основі фотонного шуму.

Таким чином, основні наукові положення, результати та висновки дисертаційної роботи достатньо повно відображені у наукових публікаціях здобувачки.

Висновок щодо відсутності (наявності) порушень вимог академічної доброчесності

За результатами ознайомлення з текстом дисертаційної роботи та наданими матеріалами ознак порушення здобувачкою вимог академічної доброчесності мною не встановлено.

У дисертації зазначено, що робота містить результати власних досліджень, а використані ідеї, результати та тексти інших авторів супроводжуються посиланнями на відповідні джерела. Наукові результати дисертації відображені у публікаціях здобувачки, а для праць у співавторстві визначено особистий внесок.

Водночас цей висновок стосується експертного аналізу наданого тексту та матеріалів і не підмінює результатів спеціалізованої перевірки текстових збігів відповідними програмними засобами.

Відповідність дисертації встановленим вимогам

Дисертація є завершеною кваліфікаційною науковою працею, у якій вирішується актуальне науково-прикладне завдання у галузі комп’ютерних наук.

Структура роботи, послідовність викладення матеріалу, оформлення результатів, наявність наукових публікацій та апробації загалом відповідають вимогам до дисертацій на здобуття ступеня доктора філософії. У висновку про наукову новизну також констатовано відповідність роботи вимогам Порядку присудження ступеня доктора філософії та вимогам щодо оформлення дисертацій.

За тематикою, об’єктом, предметом, використаними методами та характером отриманих результатів дисертаційна робота відповідає спеціальності 122 «Комп’ютерні науки».

Дискусійні положення та зауваження по дисертаційній роботі

Загалом позитивно оцінюючи дисертаційну роботу Горелікової Т. О., її наукові результати та практичну спрямованість, варто зазначити окремі дискусійні положення й зауваження.

1. У роботі достатньо детально розглянуто окремі типи атак, зокрема атаку «51%», подвійне витрачання, маніпулювання контрольними точками та змову вузлів, а в математичній моделі основним критерієм компрометації прийнято формування більшості зловмисних вузлів серед обраних валідаторів. Разом із тим, модель загроз доцільно було б формалізувати більш чітко, визначивши припущення щодо можливостей потенційного зловмисника: характеру компрометації вузлів, можливості адаптивного вибору цілей після визначення складу валідаторів, впливу на джерело випадковості та мережеву взаємодію. Це дозволило б точніше окреслити межі, у яких отримані оцінки ймовірності компрометації можуть бути поширені на різні сценарії атак.
2. У математичній моделі для врахування статистичної залежності між послідовними виборами валідаторів вводиться ефективний розмір вибірки k_eff, після чого цей показник використовується при оцінюванні ймовірності компрометації. Такий спосіб коригування є зрозумілим з погляду логіки моделі, однак у роботі доцільно було б докладніше обґрунтувати саме функціональну форму залежності k_eff від коефіцієнта кореляції та визначити умови її застосовності. Це особливо важливо з огляду на те, що на основі цієї залежності формулюються подальші висновки щодо впливу якості джерела випадковості на безпеку консенсусу.
3. Окремі кількісні висновки доцільно формулювати із зазначенням параметрів модельного сценарію, для якого вони отримані. Зокрема, твердження про збільшення ризику компрометації у 2–5 разів при певних значеннях кореляції та про гарантовану компрометацію при rho>0,3 можуть сприйматися як універсальні характеристики блокчейн-систем, хоча значення P_comp визначається також часткою зловмисних вузлів, кількістю валідаторів та іншими параметрами моделі. Доцільніше було б чіткіше пов'язати такі граничні значення з конкретними умовами проведеного чисельного експерименту.
4. Порівняльне дослідження QRNG, CSPRNG та PRNG є важливою складовою роботи, однак окремі узагальнення щодо переваг QRNG сформульовано категорично. Отримані результати переконливо демонструють високі статистичні характеристики розробленого джерела ентропії та його позитивний вплив на досліджуваний механізм рандомізованої валідації. Водночас статистична якість випадкової послідовності сама по собі не є достатньою підставою для загального висновку про криптографічну перевагу QRNG над будь-яким коректно реалізованим CSPRNG. Тому висновки щодо переваг різних типів генераторів доцільно було б чіткіше

обмежити умовами проведених експериментів і використаними реалізаціями генераторів.

5. Експериментальна частина дисертації є достатньо розгорнутою: авторкою проведено дослідження у контрольованому контейнеризованому середовищі, виконано серії тестів безпеки, продуктивності, енергоспоживання та масштабованості. Водночас наведені результати характеризують передусім розроблене експериментальне середовище та обрані конфігурації мережі. Сама авторка зазначає, що абсолютні значення показників у реальних умовах можуть відрізнятися. У зв'язку з цим, перспективним напрямом продовження роботи є верифікація запропонованого механізму в умовах реальної або загальнодоступної блокчейн-платформи з порівнянням за однакових апаратних, програмних і мережевих умов.

6. У формулюваннях наукової новизни окремі положення мають дещо ширший характер, ніж безпосередньо підтверджено проведеним дослідженням. Зокрема, твердження щодо принципово нового рівня безпеки та загального взаємозв'язку між якістю джерела ентропії і захищеністю блокчейн-систем доцільно конкретизувати стосовно запропонованого механізму рандомізованого вибору валідаторів. На мою думку, це не зменшує наукової цінності отриманих результатів, а, навпаки, дозволяє більш точно визначити авторський внесок: розроблення комплексного механізму рандомізованої валідації, його математичну формалізацію та дослідження впливу характеристик випадковості на ймовірність компрометації в межах запропонованої моделі.

Наведені зауваження мають дискусійний і рекомендаційний характер, стосуються уточнення меж застосовності окремих положень і напрямів подальшого розвитку дослідження та не впливають на загальну позитивну оцінку дисертаційної роботи.

Загальний висновок

Дисертаційна робота Горелікової Тетяни Олексіївни «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну» є завершеним самостійним науковим дослідженням, у якому отримано нові науково обґрунтовані результати щодо розроблення та дослідження методів захисту інформації у блокчейн-системах на основі рандомізованої валідації та використання високоякісних джерел ентропії.

Наукові положення та результати дисертації мають теоретичне і практичне значення для розвитку методів забезпечення цілісності та достовірності інформації у розподілених системах. Основні результати роботи опубліковано у наукових виданнях та апробовано на наукових конференціях.

За актуальністю теми, ступенем обґрунтованості наукових положень, науковою новизною, теоретичною та практичною цінністю отриманих результатів, повнотою їх опублікування та загальним рівнем виконання дисертаційна робота Горелікової Т. О. відповідає вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії, а її авторка заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 «Комп’ютерні науки».

ОФІЦІЙНИЙ ОПОНЕНТ:
Кандидат технічних наук, доцент, доцент кафедри комп’ютерних наук Київського національного економічного університету ім. В.Гетьмана — Л.В. Васильєва