Рецензія
на кваліфікаційну роботу студента
Фізико-технічного інституту «КПІ ім. Ігоря Сікорського»
Коломійця Андрія Юрійовича,
виконану на тему
«Побудова оцінки імовірності атаки подвійної витрати у протоколі консенсусу PoS за наявності чекпоінтів»

Технологія блокчейн є досить популярною в сучасності. Використання цієї технології є набагато ширшим, ніж криптовалюти, зокрема, вона дозволяє здійснювати транзакції у повністю децентралізованій системі, причому в умовах повної недовіри. Але навіть в таких системах є свої вразливості, схильність до певного роду атак на консенсусні протоколи.

Найпоширенішою атакою на блокчейн з протоколом консенсусу PoS є атака подвійної витрати. На сьогодні існують результати, що оцінюють імовірність цієї атаки, але за умови, що час її виконання є необмеженим. Проте подібну атаку з механізмом обмеження по часу ще ніхто не досліджував, й невідомо, чи покращить безпеку блокчейну даний механізм. Питання оцінки ймовірності атаки подвійної витрати в протоколі PoS за наявності контрольних точок, в яких синхронізуватиметься історія блокчейну, залишається актуальним. Саме це питання вирішується у даній дипломній роботі.

Робота Коломійця А.Ю. складається із 3 розділів. У першому розділі подано загальні теоретичні відомості про особливості технології блокчейн та типи атак. У другому розділі надано математичні описи атаки подвійної витрати. В третьому розділі наведено математичний опис в умовах обмеженого часу атаки, наведено результати обчислювального експерименту.

В представленій на рецензію роботі здійснено оцінку імовірності атаки подвійної витрати у протоколі PoS за наявності чекпоінтів, а також реалізовано математично-комп’ютерні розрахунки імовірності за отриманою формулою для різних параметрів мережі. Практичні результати дали змогу прийти до висновку, що отримана оцінка ймовірності розглянутої атаки близька за своїми значеннями з класичною оцінкою імовірності для атаки подвійної витрати у протоколі консенсусу PoS без механізму контрольних точок, якщо відстані між чекпоінтами є достатньо великими. Подібні математичні результати за даною темою дослідження було отримано вперше, і вони є підгрунтям для нових ідей досліджень в області технології блокчейн.

В роботі присутні несуттєві недоліки, зокрема, заокруглення малих ймовірностей, тоді як їх можна було б обчислити більш точно, збільшивши кількість знаків після коми. Ці особливості не впливають на загальну цінність роботи.

Зміст роботи відповідає поставленій меті, задачі дослідження повністю розв’язані. Матеріал роботи викладено чітко та логічно, за обсягом, змістом та одержаними результатами робота відповідає вимогам, що висуваються до бакалаврських дипломних робіт. Автор роботи продемонстрував компетентності, які вимагаються стандартом вищої освіти за спеціальністю “Прикладна математика”.

Вважаю, що робота «Побудова оцінки імовірності атаки подвійної витрати у протоколі PoS за наявності чекпоінтів» заслуговує оцінки «відмінно», а її автор, Коломієць Андрій Юрійович, – присудження ступеня «бакалавр» за спеціальністю 113 «Прикладна математика».

Рецензент

Доцент кафедри ІБ, к.т.н. Ірина СТЬОПОЧКІНА