ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного технічного
університету України
“Київський політехнічний інститут
імені Ігоря Сікорського”
к.філос.н., проф.
Анатолій МЕЛЬНИЧЕНКО
“8” травня 2024 р.

ВИТЯГ

з протоколу № 15 від 25 квітня 2024 р. розширеного засідання
кафедри кафедри інформатики та програмної інженерії
Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”

БУЛИ ПРИСУТНІ:

- з кафедри інформатики та програмної інженерії: завідувач кафедри, д.т.н., професор Жаріков Е.В., професор кафедри, д.т.н., професор Павлов О.А., професор кафедри, д.т.н., професор Сидоров М.О., професор кафедри, д.т.н., професор Стеценко І.В., доцент кафедри, к.т.н., доцент Ліщук К.І., доцент кафедри, к.т.н., доцент кафедри, к.т.н., доцент Фіногенов О.Д., доцент кафедри, к.т.н., доцент Лісовиченко О.І., доцент кафедри, к.т.н., доцент Баклан І.В., доцент кафедри, к.т.н. Олійник Ю.О., доцент кафедри, к.т.н., доцент Ліхоузова Т.А., доцент кафедри, к.т.н., доцент Крамар Ю.М., доцент кафедри, к.т.н., доцент Новінський В.П., асист. кафедри, д.ф. Стельмах О.П., доцент кафедри, к.т.н. Сирота О.П., доцент кафедри, к.е.н. Родіонов П.Ю., ст. викл. Вітковська І.І., ст. викл. Головченко М.М., ст. викл. Ковтунець О.В., ст. викл. Марченко О.І., аспіранти кафедри;
- з кафедри інформаційних систем та технологій: доцент кафедри, к.ф.-м.н., доцент Гавриленко О. В.;
- з інших кафедр КПІ ім. Ігоря Сікорського: завідувач кафедри програмного забезпечення комп’ютерних систем, д.т.н., доцент Сулема Є.С.;

СЛУХАЛИ:

1. Повідомлення аспіранта кафедри інформатики та програмної інженерії Колісніченка Вадима Юрійовича за матеріалами дисертаційної роботи “Методи та програмні засоби аналізу блокчейн транзакцій”, поданої на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні

здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 121 – Інженерія програмного забезпечення. Освітньо-наукова програма Інженерія програмного забезпечення.

Тему дисертаційної роботи "Методи та програмні засоби аналізу блокчейн транзакцій" затверджено на засіданні Вченої ради факультету інформатики та обчислювальної техніки (протокол № 3 від "29" жовтня 2018 року) та перезатверджено на засіданні Вченої ради факультету інформатики та обчислювальної техніки (протокол № 1 від "31" серпня 2023 року).

Науковим керівником затверджений д.т.н., доцент Дорогий Я. Ю.

2. Запитання до здобувача.
Запитання по темі дисертації ставили:
д.т.н., професор, Жаріков Е. В.
д.т.н., доцент Сулема Є.С
к.ф.-м.н., доцент, Гавриленко О. В.
к.т.н., доцент, Олійник О. А.
к.т.н., доцент, Лісовиченко О. І.
д.т.н., професор, Павлов О. А.
д.т.н., професор, Стеценко І. В.

3. Виступи за обговореною роботою.
В обговоренні дисертації взяли участь:
д.т.н., професор, Жаріков Е. В.
д.т.н., доцент Сулема Є.С
к.ф.-м.н., доцент, Гавриленко О. В.
к.т.н., доцент, Олійник О. А.
к.т.н., доцент, Лісовиченко О. І.
д.т.н., професор, Павлов О. А.
д.т.н., професор, Стеценко І. В.

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження:

1. Актуальність теми дослідження

Аналіз блокчейн мереж, а саме, блокчейн транзакцій є важливою задачею в блокчейн індустрії. У цьому контексті, зосередження уваги на блокчейн транзакціях є не лише академічним інтересом, але й практичною необхідністю для забезпечення безпеки, ефективності та стійкості мережі.

Розробники постійно працюють над відлагодженням роботи блокчейн-вузлів, що є надзвичайно важливим для підтримки надійності мережі. Це включає в себе не тільки виявлення та усунення помилок у коді,

але й оптимізацію продуктивності та масштабованості. В такому контексті, аналіз транзакцій допомагає ідентифікувати та вирішувати проблеми, які можуть впливати на роботу вузлів.

Дослідники використовують аналіз транзакцій для виявлення потенційно неефективних місць у мережі. Це включає в себе вивчення шаблонів трафіку, обробку запитів, а також аналіз затримок і пропускної здатності. Такий аналіз може виявити вузькі місця, що потребують оптимізації, або навіть передбачити потенційні проблеми, які можуть виникнути в майбутньому.

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

2. Зв'язок роботи з науковими програмами, планами, темами

Тема дисертаційної роботи відповідає планам науково-дослідної та навчальної роботи кафедри інформатики та програмної інженерії Національного технічного університету України «Київський політехнічний інститут». Дисертаційна робота розпочата на кафедрі інформаційних систем та технологій, завершена на кафедрі інформатики та програмної інженерії Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» і виконувалась в рамках наступної НДР: «Хмарна платформа розроблення і управління функціонуванням критичних IT-інфраструктур, що опрацьовують великі обсяги даних» (номер державної реєстрації № 0220U100804).

3. Наукова новизна отриманих результатів

У дисертації вперше одержані такі нові наукові результати:

– Вперше розроблено архітектуру програмного забезпечення системи аналізу транзакцій блокчейн-мереж, яка відрізняється від існуючих застосуванням принципу інверсії керування, де компоненти аналізу окремих мереж ініціюють зв’язок та самостійно надсилають дані до ядра системи, що надає можливість інтеграції нових блокчейн-мереж та методів аналізу до системи.

– Вдосконалено метод отримання даних з блокчейн-мереж, який на відміну від наявних способів прямого отримання даних з вузлів, передбачає застосування блокчейн-провідників, що надає можливість отримувати офчейн дані, які зберігаються провідником, а також уникнути розгортання власних блокчейн-вузлів під час аналізу різних мереж.

– Вперше здійснено формалізацію протоколу Peer Discovery блокчейн-мережі Rootstock на основі аналізу вихідного коду вузла RSKj, яка на відміну від інших включає та описує формати та послідовності

повідомлень, що надає можливості для реалізації незалежних клієнтів мережі, подальшого аналізу та оптимізації даної децентралізованої системи.

– Вперше розроблено метод обходу вузлів блокчейн-мереж, який відрізняється від вже існуючих методів можливістю роботи з блокчейн-мережею Rootstock, що дозволяє шляхом її представлення у вигляді орієнтованого графа та послідовного опитування кожного нового виявленого вузла отримати усі доступні блокчейн вузли мережі Rootstock та її структуру.

– Вперше розроблено метод визначення відправника транзакцій у блокчейн-мережі Rootstock через підключення до кожного знайденого вузла та аналізу часу отримання нових транзакцій, який на відміну від аналогічних методів враховує та використовує особливості мережі Rootstock, що надає можливість ідентифікувати вузол (отримати ідентифікатор та IP-адресу), який першим транслював транзакцію.

– Вдосконалено методологію аналізу транзакцій блокчейн-мережі Bitcoin, що на відміну від наявних підходів дозволяє автоматично виділяти різні типи OP_RETURN-скриптів на основі частоти появи їх префіксних частин та без попереднього знання форматів, що надає можливість розпізнавати та класифікувати дані, що зберігаються або протоколи, які побудовані з використанням OP_RETURN-скриптів.

4. Теоретичне та практичне значення результатів роботи, впровадження

Запропоновані методи та прототипи дозволяють підвищити ефективність аналізу блокчейн транзакцій у різних сферах, таких як розробка блокчейн систем, аудит смарт контрактів, розслідування злочинів пов'язаних з блокчейн мережами, трейдинг та інше.

Запропоновані методи та програмні реалізації використовуються підприємством RootstockLabs (раніше IOV Labs) для аналізу динаміки вузлів, стану мережі, та аналізу безпеки блокчейну Rootstock.

5. Апробація результатів дисертації

Основні положення і результати дисертаційної роботи обговорено на підприємстві RootstockLabs. Здобувач доповів отримані результати й отримав схвалення.

6. Дотримання принципів академічної доброчесності

За результатами науково-технічної експертизи дисертація Колісніченка Вадима Юрійовича визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 4 наукові публікації, у тому числі:

- 1 стаття у науковому фаховому виданні України за спеціальністю 121 Інженерія програмного забезпечення;

- 1 стаття у періодичному науковому виданні проіндексованому у базі Scopus;

- 2 статті у періодичних наукових виданнях проіндексованих у базах Scopus у квартилі Q3;

1. Дорогий Я. Ю., Колісніченко В.Ю. "Застосування логування у різних учасниках блокчейн-мереж для деанонімізації кінцевого користувача". Вісник Хмельницького національного університету. Серія: «Технічні науки». Номер: №5, 2023 (325). Сторінки: 60-66. ISSN 2307-5732.

Особистий внесок користувача – аналіз вихідного коду блокчейн вузлів, структуризація їх типів, аналіз методів деанонімізації,

2. Dorogyy, Y., & Kolisnichenko, V. (2023). Devising a method for rapid data retrieval using explorers for blockchain analysis. Eastern-European Journal of Enterprise Technologies, Vol. 4 No. 2 (124), 6–16. ISSN (print) 1729-3774, ISSN (on-line) 1729-4061.

Особистий внесок користувача – аналіз блокчейн експлорерів, розробка та реалізація алгоритму, проведення експерименту.

3. Dorogyy, Y., & Kolisnichenko, V. (2023). Blockchain Transaction Analysis: A Comprehensive Review of Applications, Tasks and Methods. System Research & Information Technologies, No 4, 37–53. ISSN 1681–6048.

Особистий внесок користувача – огляд існуючих систем, методів та засобів аналізу блокчейн мереж, їх структуризація.

4. Dorogyy, Y., & Kolisnichenko, V. (2024). Developing a method for the detection and identification of rootstock blockchain network nodes. Eastern-European Journal of Enterprise Technologies, Vol. 1 No. 2 (127), 6–15. ISSN (print) 1729-3774, ISSN (on-line) 1729-4061.

Особистий внесок користувача – аналіз протоколу Peer Discovery за допомогою ручного огляду вихідного коду програмного забезпечення, розробка алгоритму виявлення вузлів, реалізація прототипу та проведення експерименту.

Якість та кількість публікацій відповідають "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".

ВВАЖАТИ, що дисертаційна робота Колісніченка Вадима Юрійовича "Методи та програмні засоби аналізу блокчейн транзакцій", що подана на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 121 – Інженерія програмного забезпечення за своїм науковим рівнем, новизною отриманих результатів, теоретичною та практичною цінністю, змістом та оформленням повністю відповідає вимогам, що пред'являють до дисертацій на здобуття ступеня доктора філософії та відповідає напрямку наукового дослідження освітньо-наукової програми КПІ ім. Ігоря Сікорського "Інженерія програмного забезпечення" зі спеціальності 121 – Інженерія програмного забезпечення.

РЕКОМЕНДУВАТИ:

1. Дисертаційну роботу “Методи та програмні засоби аналізу блокчейн транзакцій”, подану Колісніченком Вадимом Юрійовичем на здобуття наукового ступеня доктора філософії, до захисту у разовій спеціалізованій вченій раді.

2. Вченій раді КПІ ім. Ігоря Сікорського утворити разову спеціалізовану вчену раду у складі:

Голова:
д.т.н., професор, декан факультету інформатики та обчислювальної техніки КПІ ім. Ігоря Сікорського Корнага Ярослав Ігорович;

Члени:
Рецензенти:
к.т.н., доцент, доцент кафедри інформатики та програмної інженерії КПІ ім. Ігоря Сікорського Олійник Юрій Олександрович;
к.ф.-м.н., доцент, доцент кафедри інформаційних систем та технологій КПІ ім. Ігоря Сікорського Гавриленко Олена Валеріївна;

Офіційні опоненти:
д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка» Опірський Іван Романович;
доктор філософії, доцент, завідувач кафедри програмної інженерії та інтелектуальних технологій управління Національного технічного університету «Харківський політехнічний інститут» Копп Андрій Михайлович.

Головуючий на засіданні
завідувач кафедри ІПІ,
д.т.н., професор — Едуард ЖАРІКОВ

Вчений секретар
кафедри ІПІ,
к.е.н., доцент — Павло РОДІОНОВ