Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0826U000693

Особливі позначки: відкрита

Дата реєстрації: 30-03-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Жикін Юрій Сергійович

2. Yurii Zhykin

Кваліфікація:

Ідентифікатор ORCID ID: 0009-0001-5930-1444

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 121

Назва наукової спеціальності: Інженерія програмного забезпечення

Галузь / галузі знань:

Освітньо-наукова програма зі спеціальності: Інженерія програмного забезпечення

Дата захисту:

Спеціальність за освітою: Інженерія програмного забезпечення

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 12375

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.23.25, 20.54.07, 27.45.17

Тема дисертації:

1. Методи та програмне забезпечення для аналізу графа Біткоїн-транзакцій

2. Methods and Software for Bitcoin Transaction Graph Analysis

Реферат:

1. За майже два десятиліття Біткоїн перетворився на важливий елемент глобальної фінансової системи – систему мікроплатежів, інвестиційний актив, інструмент міжнародних розрахунків і складову державних фінансових стратегій. Його незалежність від державних та банківських інституцій особливо приваблює користувачів із нестабільних регіонів. За таких умов анонімність і захист персональних даних набувають критичного значення. Попри це, Біткоїн не є абсолютно анонімним: відкритий реєстр транзакцій фіксує всю історію операцій, а кожен користувач представлений псевдонімними адресами. Аналіз графа транзакцій дає змогу встановлювати соціально-економічні зв'язки між учасниками, кластеризувати адреси одного користувача та здійснювати деанонімізацію, що може бути корисним у сфері правоохоронної діяльності, але становить загрозу для приватності персональних даних користувачів. Дослідження методів аналізу графа Біткоїн-транзакцій виявляє слабкі місця в моделі приватності Біткоїна і стимулює розробку інструментів

захисту. Мета роботи: спрощення процесів розроблення та експлуатації програмного забезпечення для аналізу графа Біткоїн-транзакцій шляхом розроблення узагальненої архітектури програмної системи на основі спеціалізованої моделі транзакційних даних, яка надає уніфікований семантичний контракт для інтеграції програмних компонентів і забезпечує масштабоване оброблення історії транзакцій. Розділ 1 розглядає історичні та економічні передумови появи Біткоїна, аналізує протокол і транзакційну модель, досліджує проблему приватності, технології деанонімізації та наявні інструменти захисту. Формулюється концепція і вимоги до програмної системи побудови й аналізу графа знань про транзакції. Розділ 2 присвячено розробленню спеціалізованої RDF-моделі Біткоїн-транзакцій для пошуку патернів типових операцій. Обґрунтовано вибір технологій представлення великих графів знань, розглянуто SPARQL як мову патернового аналізу з підтримкою спеціалізованих фільтр-функцій. Розділ 3 пропонує метод кластеризації виходів транзакцій на основі евристичних патернів і пропагації зв'язків власності в RDF-графі знань. Показано можливість інкрементальної кластеризації зі збереженням проміжних результатів. Сформульовано підходи до захисту від патернового аналізу: рандомізація стратегій менеджменту виходів і багатокрокова симуляція платежів одному отримувачу для маскування операцій консолідації. Розділ 4 описує архітектуру програмної системи, що складається з модулів збору даних, ETL-інструментів, RDF-сховища, компонента пропагації зв'язків та інтерфейсу дослідження графа. Розроблено процес завантаження блоків із підтримкою реорганізацій ланцюга; створено і відкрито бібліотеку для взаємодії з Біткоїн-мережею з середовища Common Lisp. Нові наукові результати: 1. Спеціалізована RDF-модель транзакційних даних, що об'єднує транзакції, їхні виходи, власників та зовнішні анотації в єдиному графі з попередньо обчисленими атрибутами, забезпечує уніфікований семантичний контракт і підтримує пошук складних багатокрокових операцій. 2. Метод інкрементальної евристичної кластеризації виходів транзакцій із покроковою пропагацією зв'язків власності та збереженням проміжних результатів у графі знань. 3. Метод захисту від патернового аналізу консолідаційних операцій шляхом багатокрокової симуляції платежів, що формує стійкий до розпізнавання підграф. 4. Узагальнена архітектура програмної системи аналізу графа транзакцій з RDF-моделлю як онтологічним ядром і стандартизованим інтерфейсом взаємодії.

2. Over nearly two decades, Bitcoin has evolved into a significant component of the global financial system – a micropayment system, investment asset, instrument for international settlements, and element of state financial strategies. Its independence from governmental and banking institutions is particularly attractive to users in unstable regions. In this context, anonymity and personal data protection become critically important. Nevertheless, Bitcoin is not fully anonymous: its open transaction ledger records the complete history of all operations, with each user represented by pseudonymous addresses. Transaction graph analysis enables the establishment of socio-economic links between participants, clustering of addresses belonging to the same user, and deanonymization – which may be valuable for law enforcement, but poses a threat to users' financial privacy. Studying Bitcoin transaction graph analysis methods reveals weaknesses in Bitcoin's privacy model and drives the development of protective tools. Objective: To simplify the development and operation of software for Bitcoin transaction graph analysis by designing a generalized software system architecture based on a specialized transaction data model that provides a unified semantic contract for component integration and ensures scalable processing of transaction history. Section 1 examines the historical and economic prerequisites for Bitcoin's emergence, analyzes the protocol and transaction model, investigates the privacy problem, deanonymization technologies, and existing protective tools. The concept and requirements for a software system for constructing and analyzing a transaction knowledge graph are formulated. Section 2 is devoted to developing a specialized RDF model of Bitcoin transactions for identifying patterns of typical operations. The choice of technologies for representing large-scale knowledge graphs is justified, and SPARQL is examined as a pattern analysis query language with support for custom filter functions. Section 3 proposes a method for clustering transaction outputs based on heuristic patterns and ownership relation propagation within an RDF knowledge graph. Incremental clustering with preservation of intermediate results is demonstrated. Approaches to protection against pattern analysis are formulated: randomization of output management strategies and multi-step payment simulation to a single recipient for masking consolidation operations. Section 4 describes the software system architecture,

consisting of data collection modules, ETL tools, an RDF store, an ownership propagation component, and a graph exploration interface. A block loading process with blockchain reorganization support is developed; a library for interacting with the Bitcoin network from the Common Lisp environment is created and released as open-source software. New scientific results: 1. A specialized RDF transaction data model that unifies transactions, their outputs, owners, and external annotations in a single graph with precomputed attributes – providing a unified semantic contract and supporting queries for complex multi-step operations. 2. A method for incremental heuristic clustering of transaction outputs with step-by-step ownership relation propagation and storage of intermediate results within the knowledge graph. 3. A method for protecting against pattern analysis of consolidation operations through multi-step payment simulation, forming a recognition-resistant subgraph. 4. A generalized software system architecture for transaction graph analysis, with the RDF model as an ontological core and a standardized interaction interface.

Державний реєстраційний номер ДіР: 0124U000907

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Жикін Ю.С. Патерновий аналіз графа Біткоїн-транзакцій. / Ю.С. Жикін, М.В. Онай // Вісник Хмельницького національного університету. Серія: Технічні науки – 2024. – №2. – С. 322-328. – DOI:10.31891/2307-5732-2024-333-2-51.
- Жикін Ю.С. RDF-модель графа Біткоїн-транзакцій. / Ю.С. Жикін, М.В. Онай // Вісник Хмельницького національного університету. Серія: Технічні науки – 2024. – №5. – С. 25-30. – DOI:10.31891/2307-5732-2024-341-5-3.
- Жикін Ю.С. Метод консолідації виходів Біткоїн-транзакцій за допомогою симуляції витрачання. / Ю.С. Жикін, М.В. Онай // Комп'ютерно-інтегровані технології: освіта, наука, виробництво – 2025. – №59. – С. 113-119. – DOI:10.36910/6775-2524-0560-2025-59-15.
- Жикін Ю.С. Метод групування адрес за власністю на основі патернів типових операцій у графі Біткоїн-транзакцій. / Ю.С. Жикін, М.В. Онай // Прикладна математика та комп'ютинг. ПМК, 2024: Сімнадцята наук. конф. магістрантів та аспірантів, Київ, 20-22 лист. 2024 р.: зб. тез доп. [редкол.: Дичка І. А. та ін.]. – К.: ПТФ «Просвіта», 2024.– С. 87-92.
- Жикін Ю.С. Метод зменшення розміру RDF-графа за допомогою непрямої типізації. / Ю.С. Жикін, М.В. Онай // Традиційні та інноваційні підходи до наукових досліджень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції (Дрогобич, 31 січня 2025 р.) / Міжнародний центр наукових досліджень. – Вінниця: ТОВ “УКРЛОГОС Груп”, 2025. – С. 287-290. – DOI:10.62731/mcnd-31.01.2025.007.
- Жикін Ю.С. Взаємодія з Біткоїн-мережею з програмного середовища Common Lisp. / Ю.С. Жикін, М.В. Онай // Наукові орієнтири: теорія та практика досліджень: збірник наукових праць з матеріалами VI Міжнародної наукової конференції (Київ, 3 жовтня 2025 р.) / Міжнародний центр наукових досліджень. – Вінниця: ТОВ “УКРЛОГОС Груп”, 2025. – С. 196-199. – DOI:10.62731/mcnd-03.10.2025.002.
- Жикін Ю.С. Узагальнена архітектура програмної системи для побудови та аналізу графа знань про Біткоїн-транзакції. / Ю.С. Жикін, М.В. Онай // Міжгалузеві диспути: динаміка та розвиток сучасних наукових досліджень: збірник наукових праць з матеріалами VIII Міжнародної наукової конференції (Харків, січень 2026 р.) / Міжнародний центр наукових досліджень. – Вінниця: ТОВ “УКРЛОГОС Груп”, 2026. – С. 229-232. – DOI:10.62731/mcnd-30.01.2026.006.

Наукова (науково-технічна) продукція: технології; методи, теорії, гіпотези; програмні продукти, програмно-технологічна документація

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впровадження не планується

Зв'язок з науковими темами: 0124U000907

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Онай Микола Володимирович
2. Mykola Onai

Кваліфікація: к. т. н., доц., 05.13.05

Ідентифікатор ORCID ID: 0000-0002-4938-8355

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Шубін Ігор Юрійович
2. Igor Y. Shubin

Кваліфікація: к.т.н., доц., 01.05.03

Ідентифікатор ORCID ID: 0000-0002-1073-023X

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Субботін Сергій Олександрович

2. Serhii O. Subbotin

Кваліфікація: д. т. н., професор, 05.13.23

Ідентифікатор ORCID ID: 0000-0001-5814-8268

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Запорізька політехніка"

Код за ЄДРПОУ: 02070849

Місцезнаходження: вул. Жуковського, Запоріжжя, Запорізький р-н., 69063, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Стеценко Інна Вячеславівна

2. Inna V. Stetsenko

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-4601-0058

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Гавриленко Олена Валеріївна

2. Olena V. Gavrilenko

Кваліфікація: к. ф.-м. н., доц., 01.02.05

Ідентифікатор ORCID ID: 0000-0003-0413-6274

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Коваль Олександр Васильович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Коваль Олександр Васильович
Відповідальний за підготовку облікових документів	Жикін Юрій Сергійович
Реєстратор	Юрченко Тетяна Анатоліївна
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна