УДК 004.043 **DOI:10.30837/rt.2021.4.207.04**

В.В. ДУБІНА, Р.В. ОЛІЙНИКОВ, д-р техн. наук

МЕТОДИ ТА ЗАСОБИ ДЕАНОНІМІЗАЦІЇ ТРАНЗАКЦІЙ В БЛОКЧЕЙН

Вступ

Забезпечення належної безпеки в комп'ютерних мережах – це основна умова захисту даних від різного виду загроз. Велика кількість факторів може мати негативний вплив на ефективне функціонування мережі. Загрози можуть з'явитися під час помилок та різних збоїв у роботі системи або внаслідок навмисних дій зловмисника, що може призвести до розголошення або втрати конфіденційних даних. Через це сучасні мережі все більш потребують належного захисту. Суттєві переваги перед стандартними підходами зберігання даних мають технології розподіленого реєстру, які сьогодні набувають широкого розповсюдження, і можуть бути ефективно використані для боротьби зі зростаючою кількістю загроз.

До такого типу мереж відноситься і технологія блокчейн. Усі її учасники знаходяться в рівному становищі і одночасно володіють всією доступною інформацією. Кожен зберігає у себе точний список операцій, які були здійснені за весь час, і будь-які зміни, внесені до реєстру, одразу будуть виявлені користувачем [1, 2]. Через це блокчейн складно атакувати, адже для того, щоб досягти успіху, зловмиснику необхідно атакувати усі копії.

Системи на основі подібних мереж набувають активного розвитку і поширення. Розробники, передбачаючи масштаби нових досягнень, почали активно створювати цифрові валюти з різними властивостями та можливостями, платформи смарт-контрактів, цифрові платформи для голосування, стійкі до шахрайства тощо [3]. Таким чином, поєднуючи усі можливості, блокчейн мережі знаходять застосування в областях, що стосуються фінансових операцій, ідентифікації користувачів або створення нових технологій кібербезпеки.

Однак водночас велика кількість можливостей блокчейн-систем часто привертає увагу зловмисників. В більшості випадків зловмисники намагаються маніпулювати процесом досягнення консенсусу, щоб змінити інформацію, що вноситься до реєстру. Тому все більше мережі, які генерують і обслуговують цифрові активи, піддаються різноманітним атакам [4], а питання відстеження підозрілої активності і своєчасного захисту користувачів мережі залишається актуальним.

Дану роботу присвячено виявленню основних властивостей технології блокчейн, дослідженню принципів обробки даних і визначенню можливих шляхів деанонімізації транзакцій, як засіб для попередження зловживання криптовалютою у мережі.

В роботі проведено аналіз сучасних блокчейн-систем, визначено актуальні проблеми технології, досліджено принципи формування і обробки транзакцій, а також на прикладі сучасних інструментів відстеження розглянуто можливі засоби аналізу блокчейн мереж, досліджено принципи обробки і властивості анонімності транзакцій у сучасних блокчейн системах.

1. Принципи формування та обробки транзакцій

Технологія блокчейн створює структуру даних з властивими її якостями безпеки. Вона заснована на принципах криптографії, децентралізації і консенсусу, які забезпечують довіру до учасників мережі і здійснених транзакцій. Як правило, в більшості технологій розподіленого реєстру дані упорядковані в блоках, і кожен з них містить одну або декілька транзакцій. Кожен новий блок підключається до усіх попередніх в криптографічний ланцюжок таким чином, що втручання стає неможливим [5]. Усі транзакції всередині блоків перевіряються і узгоджуються за допомогою механізму консенсусу, який гарантує, що кожна транзакція підтверджена більшістю валідаторів. Жоден користувач в мережі не може змінити запис транзакцій [2].

В залежності від алгоритму консенсусу обраної блокчейн-системи визначаються й певні особливості процесу видобутку блоків, адже від нього залежать такі характеристики, як: швидкість створення блоку, розмір ланцюжка блоків, обсяг середньої відправленої транзакції, швидкість підтвердження та інше. Але перш за все необхідно розібратися з тим, що представляє собою транзакція всередині блокчейн-мережі.

Під поняттям транзакції розуміють передачу криптовалюти або будь-якої іншої інформації з однієї адреси на іншу. При цьому, на відміну від банківських транзакцій, реального фізичного об'єкту передачі не існує, користувачі отримують криптовалюту через транзакцію і витрачають так само.

Пріоритет попадання операцій в новий блок наступний [6]:

1) персональні операції власників пулу;

2) розподіл прибутку на гаманці майнерів;

3) комерційні операції.

Процес перевірки та запису є негайним і неперервним. Користувач вказує адресу одержувача і кількість валюти, яку хоче відправити, та завіряє відправку транзакції своїм ключем. Відразу ж після цього транзакція надходить в пов'язане з гаманцем ядро і зберігається спеціальній зоні для непідтверджених транзакцій, що називається мемпулом. Якщо обрана з них транзакція буде схвалена більшістю вузлів, то вона записується в блок. Кожен блок містить перелік всіх транзакцій з відміткою часу та геш кожного попереднього блоку, завдяки якому їх можна розрізняти між собою, створивши безперервний ланцюжок. Для обробки кожного наступного блоку майнерам необхідно підтверджувати попередні транзакції, записані в більш ранніх блоках ланцюжка. Чим більше транзакція їх отримає, тим більш надійною вона буде вважатися. Після обробки і появи в блокчейн реєстрі транзакція вважається дійсною.

Транзакції у системі є публічними, тому усі учасники мережі мають змогу відстежувати весь потік криптовалюти, що надсилається між адресами. Однак більшість власників криптоактивів не бажають, щоб історії їх транзакцій і інформація облікового запису розкривалися іншим [1]. Як правило, користувачі не здатні виявити ніякі чужі особисті дані, адже кожній новій транзакції надається новий номер, що являє собою набір випадкових цифр. Він є свого роду захистом від небажаного втручання та ускладненням для атак [7]. Але у випадку, якщо навіть одна з транзакцій стане ідентифікованою і буде визначений її власник, то існує ймовірність, що окрім його історії переведень й власники інших транзакцій стануть відомі також.

Наявність проблеми, що полягає у відсутності повної конфіденційності, стало поштовхом для розробки нових анонімних платіжних блокчейн систем [1][8]. Найвідомішими прикладами таких криптовалют є: Monero, Dash, Zcash тощо [9]. Таким чином, анонімна або орієнтована на конфіденційність монета – це різновид криптовалют, головною метою яких є збереження приватності своїх користувачів.

На сьогодні існує декілька шляхів щодо підвищення анонімності у мережі блокчейн. Перша технологія заснована на змішуванні монет, ідея якої полягає в поєднанні кількох платежів в одну транзакцію, після чого розподіл коштів з пулу відбувається між відповідним одержувачами [1], друга – технологія доказів, заснованих на поліномах, такі як доказ з нульовим розголошенням – Zero-Knowledge Proof, який дозволяє зберігати і обмінюватися даними в захищеному вигляді, гарантуючи невтручання в процес комунікації третіх осіб.

Таким чином, анонімні транзакції є чудовим рішенням у забезпеченні конфіденційності учасників мережі. Це безумовне право користувачів, які бажають зберегти свої дії у секреті. Однак у той же час потрібно пам'ятати, що наявність такої анонімності в системі сьогодні все частіше стає приводом для проведення фінансових махінацій у мережі. У зв'язку з цим з'явилася необхідність в контролі за діями у блокчейн мережах та вдосконаленні усіх існуючих на даний час аспектів кіберзахисту.

2. Методи деанонімізації транзакцій

Дослідження деанонімізації криптовалют можна виконати двома засобами. Першим з них є аналіз ланцюжка транзакцій за допомогою відповідних мережевих інструментів, який полягає у відстеженні транзакцій по мережі та накопиченні загальнодоступних відомостей про них, а також пов'язуванні їх з особистими даними користувача [10]. Інший метод – це аналіз протоколу та мережі, який використовує характеристики розповсюдження транзакцій з криптовалютою для визначення вихідної IP-адреси нової транзакції [11, 12].

На сьогодні можна обирати серед комерційних послуг та інструментів з відкритим кодом, що забезпечують програмний доступ. Для відстеження шляху переміщення транзакцій до кінцевого одержувача дозволяють провести розглянуті далі сервіси.

Blockchain Explorer [13] – це один з найбільш відомих інструментів аналізу ланцюжка блоків. Він пропонує ряд можливостей для відстеження окремих транзакцій, а також надає інформацію у вигляді графіків і статистики всієї мережі. Крім того, з його допомогою можна провести аналіз стосовно руху коштів по мережі. На головній сторінці сервісу можемо побачити діаграми, що відображають зміни цін на криптовалюту за останній день, тиждень або місяць, а також сумарний розмір непідтверджених транзакцій в байтах. Крім того, маємо можливість детального перегляду інформації, що надає нам ще більшу кількість діаграм, які побудовані за валютною статистикою, деталями блоку, інформацією про їх видобуток, мережевою активністю, кількістю активних гаманців, а також ринковими сигналами. Також тут нам одразу відомі які і ким були отримані останні блоки, їх розмір, а також список непідтверджених транзакцій та суми, які були передані. Відображені відомості також можна розглянути детальніше і дізнатися час передачі окремої транзакції в мережу, комісію, яка була сплачена за її обробку, розмір транзакції, перелік адрес і сум з витраченими і отриманими коштами.

Matbea.net [14] – це послуга, яка дозволяє користувачам встановлювати належність біткоїн-адрес. Даний інструмент надає користувачам можливість шукати інформацію по транзакціям, адресам, блокам, xPub або yPub і видає результат у вигляді детальної текстової статистики. Послуга перекладена на кілька іноземних мов та має зрозумілий інтерфейс.

ORS CryptoHound [15] – це ще один інструмент дослідження мережі на базі штучного інтелекту, який використовується для дослідження Біткоїн та Ефіріум адрес і надає результати у вигляді списків, діаграм або таблиць. Інструмент пропонує можливості відстеження коштів за конкретною адресою, відображення залишку на балансі, візуалізацію відношень адрес і всіх транзакцій, що проведені нею, дозволяє виконувати статистичний розрахунок вартості монет, а також формування банківських звітів.

Сервіс Glassnode [16] являє собою аналітичну компанію, що займається аналітикою блокчейн мереж і надає оперативну інформацію про стан ринку, пропонуючи відображення результатів в різних категоріях.

Використання подібних інструментів з відкритим кодом є досить зручним за рахунок їх доступності, однак деякі з них вимагають багато часу для дослідження окремих ділянок мережі та транзакцій і проводити такий аналіз вручну стає неефективним. До того ж, щоб вчасно виявити загрозу і попередити атаки, необхідно мати здатність передбачення методів, які можуть застосувати зловмисники в мережі.

3. Відстеження транзакцій з використанням платформи GraphSense

Усі основні методи деанонімізації поєднала у собі система GraphSense Cryptoasset Analytics. Інструмент дозволяє реалізовувати пошук серед криптовалютних адрес, блоків, транзакцій та тегів, а також виявляти кластери, пов'язані з певною адресою. Цей проєкт розроблений австрійськими дослідниками, з метою допомогти користувачам відслідкувати переміщення коштів у мережі і виявити будь-які аномалії. Даний інструмент поєднує у собі можливості сучасних комерційних варіантів аналітики мереж та загальнодоступних з відкритим кодом [17]. GraphSense надає панель інструментів для базових досліджень мережі та

забезпечує гнучкість для виконання дослідницьких задач з наданням обчислень у вигляді графів. Система являє собою платформу для аналізу криптоактивів з забезпеченням повної незалежності даних, алгоритмічної прозорості та масштабованості. GraphSense має відкритий вихідний код і є безкоштовним. Окрім цього, надає інформаційну панель Dashboard для мережевих досліджень і, що є найголовнішим, повний контроль даних для виконання розширених завдань аналітики [18].

Під поняттям активу розуміємо економічний ресурс, що має певну цінність для користувача. Криптоактив, у свою чергу, це призначений для обміну віртуальний актив із використанням криптографії. Розрізняють такі види криптоактивів, як: власні криптовалюти (Native Cryptocurrencies), гарним прикладом яких є платіжна система Bitcoin і токени (Tokens), що розгорнуті на таких платформах, як Ethereum. З точки зору використання можна визначити токени оплати (Payment Tokens), токени безпеки (Security Tokens) і службові токени (Utility Tokens) [17].

Система проводить аналіз транзакцій в мережі у реальному часі, щоб отримати уявлення про їх функції і статистику. Особлива увага приділяється виявленню так званих аномалій, тобто ідентифікації тих транзакцій, які відхиляються від стандартних структур. Це дозволяє виявляти і відстежувати потенційно зловмисні дії на ранніх стадіях.

Інструмент має ряд особливостей, такі як [18]:

- можливість міжвалютного пошуку у системі за адресою, тегом, транзакцією або блоком у декількох регістрах криптовалюти;
- перевірка метаданих, властивостей вузлів та їх взаємодії;
- перегляд та переміщення по транзакціям, виявлених з різних реєстрів;
- підтримка аналітики на основі даних через REST API;
- автоматичний пошук шляхів транзакцій, які з'єднують два вузли;
- механізми Apache Spark та Cassandra в основі, задля досягнення лінійної масштабованості;
- використання інструменту BlockSci для аналізу ланцюжків блоків та фільтрації CoinJoins;
- програмне забезпечення є відкритим і має ліцензію MIT.

GraphSense надає можливість працювати з такими криптовалютами, як: Bitcoin, Bitcoin Cash, Ethereum, Litecoin і Zcash, а також іншими валютами моделі UTXO [5] [17].

Візуальна панель управління Dashboard працює у будь-якому сучасному веб-браузері і дозволяє виконувати перевірку блоків, транзакцій, адрес та сутностей, а також навігацію по ним. Таким чином, користувачі можуть відстежувати грошові потоки та будувати графи за результатами їхніх досліджень [17].

В процесі введення символів у поле пошуку система сама генерує можливі варіанти. Після того як ввели бажані дані для пошуку, на панелі управління з'являється графічне відображення питомої адреси у вигляді блоку, де відображається кількість відношень на вхідній та вихідній сторонах, а також завантажений суб'єкт для цієї адреси, який контролює кластером з 12 адрес, що обчислено методом кластеризації (рис. 1).

Address	First usage	Last usage	Final balance	Total received
122x97UkuMsT6hNQnDs3ytYwsKaPreQ4cK	03/25/2017 6:10:40 PM	03/26/2017 2:29:54 AM	0 BTC	0.0116 BTC
13wDiidMjFhcrd75zRkN6DNjBbMmetHZjq	03/26/2017 2:29:54 AM	03/29/2017 9:41:47 AM	0 BTC	5.9574 BTC
169rGApQW68tiprsy851tCZ6ACmLnmXkj4	07/26/2018 5:59:22 PM	07/29/2018 10:10:05 PM	0 BTC	0.15 BTC
✔ 18NSAybFEhLa6AG3gxEN1hiaRJoSvvbnDb	12/15/2016 4:37:11 AM	01/20/2020 3:43:06 PM	0 BTC	14.3924 BTC
19yijwxaFSzQ11GNeBHwpAYv29qJt2e4wT	10/02/2018 5:30:09 AM	01/06/2020 10:51:32 PM	0 BTC	0.9848 BTC
1AR3DiQftXZCNEGyhMg1kRs83tr2Ao6J1Z	12/17/2017 10:33:41 PM	01/06/2020 10:51:32 PM	0 BTC	0.0983 BTC
1JPeBHn5pYVudEFvgPqjpq9pbjdsAAR3vC	08/22/2017 5:09:50 AM	01/06/2020 10:51:32 PM	0 BTC	0.0077 BTC
1MupxiyR1HuGMrGU4trLxFwaRyRDm2W5gx	07/29/2018 10:10:05 PM	01/06/2020 10:51:32 PM	0	

Showing 1 to 9 of 12 entries

Рис. 1. Кластер адрес

Задача кластеризації полягає в ідентифікації схожих адрес, які при цьому є окремими входами однієї транзакції, і додаванні їх в одну групу, визначивши як ті, що належать одному власнику [19].

Також сервіс завантажує детальну статистику підключеної адреси, яка відображає інформацію про кількість проведених транзакцій, в яких адреса використовувалась в якості введення або виведення, кількість адрес, з яких було отримано та надіслано монети, дати першого та останнього використання, період активності та суму отриманих коштів, значення яких також можна конвертувати між валютами долара або євро. В цьому ж вікні можемо переглянути перелік проведених транзакцій, вхідних та вихідних адрес у вигляді таблиць (рис. 2). Також є можливість провести пошук окремої транзакції або адреси зі списку за необхідністю.

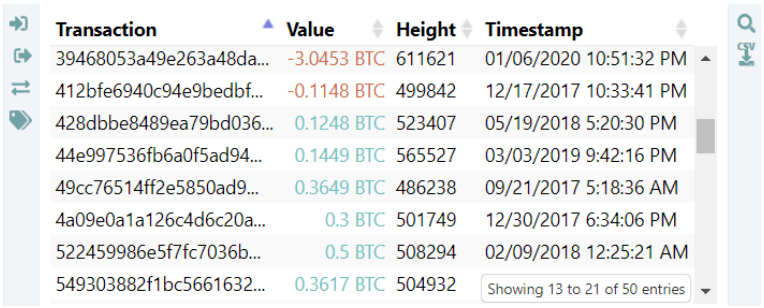

Рис. 2. Перелік проведених транзакцій

Платформа GraphSense надає можливість додатково дослідити кожне вхідне та вихідне відношення за допомогою побудови адресних графів і їх сутностей з усіма деталями. Можна обрати будь-яку адресу з таблиць і додати її до існуючого блоку (рис. 3).

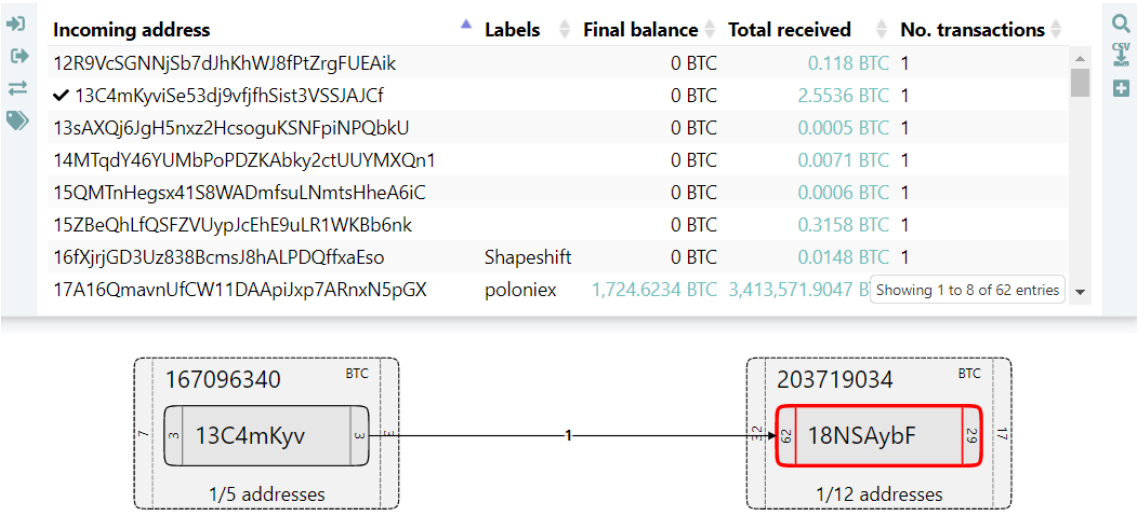

Рис. 3. Відображення вхідного відношення

Обравши транзакцію для детального перегляду можна дізнатися до якого блоку її було включено, час і дату її проведення, суму, яка була надіслана, побачити її джерело і призначення, тобто усі вихідні адреси, на які вона була надіслана.

Аналізуючи перелік транзакцій, як на вхідній, так і на вихідній сторонах, можна побачити, що існують адреси з відповідними мітками. Це теги, що є спільним позначенням адрес та сутностей криптоактивів деяких реальних комерційних організацій, таких як криптовалютні біржі, майнінг-пули та інші (рис. 4).

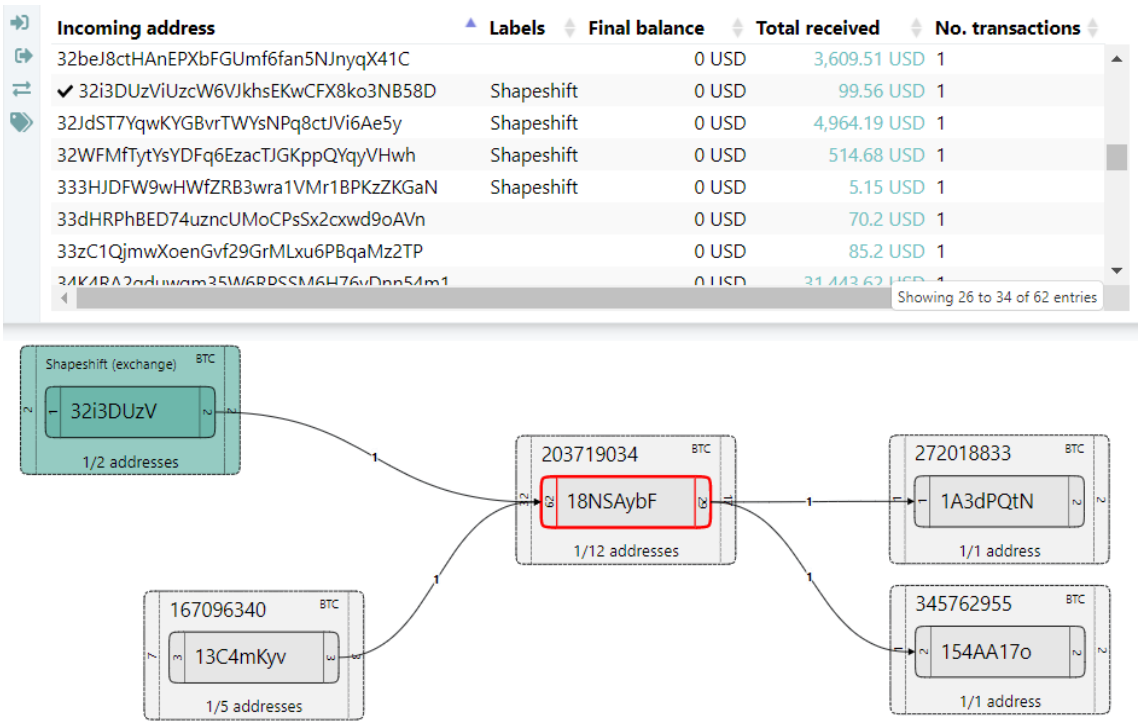

Рис. 4. Тегування адрес

Тегування є важливою функцією, адже, взаємодіючи з певними службами та призначаючи їх адресам зручні для обробки мітки, можна ідентифікувати клієнтів як ті, що належать і керуються відомими криптовалютними організаціями, групувати їх за відповідними тегами та категоріями і проводити ефективний аналіз мережі, відстежуючи операції відомих учасників. Платформа GraphSense використовує для цього файлову структуру TagPacks.

Даний інструмент є зручним у використанні, при цьому він пропонує велику кількість можливостей з високим рівнем ефективності, дозволяючи його користувачам отримувати статистику за запитом за досить швидкий час.

В перспективі, продовжуючи вдосконалення платформи і забезпечуючи зростаючий набір її функцій, GraphSense може стати гарним інструментом для тих підприємств і організацій, що займаються криптоактивами, для наукових досліджень, а також можливим вирішенням виникаючих проблеми щодо дотримання та регулювання безпечних відносин у Блокчейн мережах.

Висновки

Транзакції в блокчейн-мережі проводяться публічно, і кожен користувач в будь-який час може переглянути їх. Це досягається за рахунок прозорості, що є однією з головних відмінних рис технології. Однак не завжди учасники бажають, щоб інформація про стан їх заощадження і історії транзакцій були повністю відомі іншим. Конфіденційність користувачів може бути збережена за рахунок анонімних транзакцій.

Анонімність транзакцій – одна з причин популярності криптовалют та широкого поширення технології блокчейн. Однак її наявність у мережі є основою виникнення нечесних транзакцій, фінансових махінацій і атак на систему. На сьогодні найбільш актуальною проблемою Блокчейн мереж є зловживання криптовалютою з метою проведення злочинних дій. Тому з'явилася необхідність у постійному контролі за діями користувачів, у зв'язку з цим почалась активна розробка інструментів аналізу мережі, які здатні відстежувати історії здійснених транзакцій. Сьогодні можна обирати між комерційними послугами аналізу та інструментами з відкритим кодом.

Існуюча методологія деанонімізації транзакцій передбачає відстеження всієї історії їх просування по мережі. Для аналізу ланцюжка і збору даних можна використовувати такі

інструменти, як: Blockchain Explorer, Matbea.net, CryptoHound, Glassnode. Зручний та ефективний сервіс GraphSense дозволяє виконувати розширені завдання аналітики в реальному часі, з результатами у вигляді графів і таблиць з усією історією транзакцій, що дозволяє додатково досліджувати кожне вхідне і вихідне відношення за допомогою побудови адресних графів і спостерігати за всім ланцюжком, виявляючи аномальну поведінку у мережі.

Список літератури:

1. Rui Zhang, Rui Xue, Ling Liu. Security and Privacy on Blockchain // ACM Computing Surveys. 2019. Vol. 52, No. 3, Article 51. 34 p.
2. Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser, 2016. 88 p.
3. Aaron Wright, Primavera De Filippi. Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 2015. 58 p.
4. Колесников П.И., Бекетнова Ю.М., Крылов Г.О. Технология блокчейн. Анализ атак, стратегии защиты. 2017. 67 p.
5. What is blockchain security? *IBM*: веб-сайт. URL: https://www.ibm.com/topics/blockchain-security
6. Transactions in the BTC blockchain. *EXMO*: веб-сайт. URL: https://info.exmo.me/en/education/transactions-in-btc-blockchain/
7. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions / M.A. Uddin and others. Blockchain: Research and Applications, 2021. 80 p.
8. Harry Halpin, Marta Piekarska. Introduction to Security and Privacy on the Blockchain. IEEE European Symposium. 2017. 3 p.
9. Бедрій Т. А., Ісмайлов К. Ю., Медведенко С. В. Використання знань про особливості криптовалют у протидії злочинності // Кібербезпека в Україні: правові та організаційні питання: матеріали III Всеукр. наук.-практ. конф. Одеса, 2018. С. 140-144.
10. Androulaki E., Karame G. O., Roeschlin M., Scherer T., & Capkun S. Evaluating user privacy in Bitcoin // Financial Cryptography and Data Security – 17th International Conference, FC 2013, Revised Selected Papers. Vol. 7859 LNCS, pp. 34-51.
11. Philip Koshy, Diana Koshy, and Patrick McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. 2014. Financial Cryptography, 2014.
12. Biryukov A., Khovratovich D., Pustogarov I. Deanonymisation of clients in Bitcoin P2P network, CoRR, Vol. abs, 2014.
13. Офіційний веб-сайт Blockchain Explorer. URL: https://www.blockchain.com/en/explorer
14. Офіційний веб-сайт Matbea.net. URL: https://matbea.net/
15. Офіційний веб-сайт ORS CryptoHound. URL: https://www.c-hound.ai/
16. Офіційний веб-сайт Glassnod. URL: https://studio.glassnode.com/
17. Bernhard Haslhofer and others. GraphSense: A General-Purpose Cryptoasset Analytics Platform. 2021. 16 p.
18. Офіційний сайт GraphSense. URL: https://graphsense.info/
19. Данильчук Р. К., Жураковська О. С. Задача кластеризації адрес в мережі Блокчейн // Міжнар. наук. журнал «Інтернаука». Київ, 2018. № 9(49). Т. 1. С. 43-46.

Надійшла до редколегії 12.10.2021

Відомості про авторів:

Дубіна Валерія Вадимівна – Харківський національний університет радіоелектроніки, магістрант, кафедра безпеки інформаційних технологій, факультет комп'ютерної інженерії та управління, Україна; email: valeriia.dubina@nure.ua; ORCID: https://orcid.org/0000-0002-8653-8025

Олійников Роман Васильович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: roman.oliinykov@nure.ua; ORCID: https://orcid.org/0000-0002-3494-0493