DOI 10.31891/2307-5732-2023-325-5-60-66
УДК 004.4+004.9

ДОРОГИЙ ЯРОСЛАВ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0003-3848-9852
e-mail: argusyk@gmail.com
КОЛІСНІЧЕНКО ВАДИМ
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0009-0009-6472-2807
e-mail: vadym.kolisnichenko@gmail.com

ЗАСТОСУВАННЯ ЛОГУВАННЯ РІЗНИМИ УЧАСНИКАМИ БЛОКЧЕЙН-МЕРЕЖ ДЛЯ ДЕАНОНІМІЗАЦІЇ КІНЦЕВОГО КОРИСТУВАЧА

Блокчейн-технології радикально переосмислили спосіб виконання фінансових транзакцій. Замість того, щоб покладатися на традиційні централізовані інституції, такі як банки або платіжні системи, транзакції тепер обробляються в децентралізованій мережі, де незалежні рівноправні вузли діють як гаранти правильності та легітимності кожної операції. Кожен вузол не тільки перевіряє легітимність блоків та транзакцій, але й додає їх до своєї власної копії ланцюга блоків – блокчейну. Ця взаємодія і взаємозалежність вузлів сприяє створенню системи, в якій обмін даними відбувається із високим рівнем довіри до їхньої автентичності та безпеки.

Однак, поряд із численними позитивними сторонами такої системи, існують і певні виклики, особливо щодо конфіденційності кінцевого користувача. Незважаючи на поширену думку, що блокчейн-мережі надають абсолютну анонімність користувачам, на практиці є численні нюанси, які дозволяють ідентифікувати кінцевого користувача, що взаємодіє з блокчейн-мережею. Тому важливо розуміти реальний рівень конфіденційності, який забезпечує блокчейн, а також знати можливі ризики деанонімізації.

Ця стаття заглиблюється у деталі блокчейн-технологій, спрямовуючи основну увагу на те, як різноманітні учасники блокчейн-мереж можуть використовувати логування для збору та аналізу даних, а саме, систематично реєструвати активності та взаємодії користувача з мережею. На перший погляд, це може здатися невинним або технічним аспектом, проте в реальності такий підхід може стати інструментом для виявлення конфіденційної інформації користувачів, та врешті-решт його деанонімізації. Тому, у світлі зростання популярності блокчейн-технологій та криптовалют, важливо зрозуміти, які можливості і ризики існують у контексті конфіденційності та анонімності.

Ключові слова: блокчейн аналіз, конфіденційність у блокчейні, деанонімізація, логування, блокчейн-вузли.

DOROGIY YAROSLAV
National technical university of ukraine "ihor sikorsky kyiv polytechnic institute".
KOLISNICHENKO VADIM
National technical university of ukraine "ihor sikorsky kyiv polytechnic institute".

APPLICATION OF LOGGING IN VARIOUS PARTICIPANTS OF BLOCKCHAIN NETWORKS FOR DE-ANONYMIZATION OF THE END USER

Blockchain technologies have radically rethought the way financial transactions are performed. Instead of relying on traditional centralized institutions such as banks or payment systems, transactions are now processed in a decentralized network where independent peer nodes act as guarantors of the correctness and legitimacy of each transaction. Each node not only verifies the legitimacy of blocks and transactions, but also adds them to its own copy of the block chain, the blockchain. This interaction and interdependence of nodes contributes to the creation of a system in which data exchange takes place with a high level of confidence in their authenticity and security.

However, along with the many positive aspects of such a system, there are also certain challenges, especially regarding the confidentiality of the end user. Despite the popular opinion that blockchain networks provide absolute anonymity to users, in practice there are numerous nuances that allow the identification of the end user interacting with the blockchain network. Therefore, it is important to understand the real level of confidentiality that blockchain provides, as well as to know the possible risks of de-anonymization.

This article delves into the details of blockchain technology, focusing on how various participants in blockchain networks can use logging to collect and analyze data, namely, to systematically record a user's activities and interactions with the network. At first glance, this may seem like an innocent or technical aspect, but in reality, such an approach can become a tool for discovering sensitive user information, and eventually de-anonymizing the end user. Therefore, considering the growing popularity of blockchain technologies and cryptocurrencies, it is important to understand what opportunities and risks exist in the context of confidentiality and anonymity.

Keywords: blockchain analysis, blockchain confidentiality, deanonymization, logging, blockchain nodes.

Вступ

Блокчейн – це децентралізована технологія цифрового реєстру, що змінила підхід до зберігання та обміну даними. У блокчейні, транзакції групуються у блоки, які поступово додаються до ланцюга в хронологічному порядку. Кожен блок містить в собі не лише інформацію про транзакції, але й хеш попереднього блока. Це створює послідовний ланцюг, в якому кожен блок підтверджує попередній та забезпечує надійність даних. Кожна окрема транзакція верифікується всіма вузлами мережі. Цей підхід дозволяє уникнути централізованих посередників та забезпечити високий рівень довіри до даних.

Важливим аспектом блокчейн-мережі є її децентралізованість, яка досягається мережею рівноправних блокчейн-вузлів. Транзакції не підлягають централізованому контролю, а замість цього, вони верифікуються

відповідно до правил блокчейн-мережі – консенсусу [1]. Кожен вузол перевіряє легітимність блоку та транзакцій, та додає їх до персональної копії ланцюга, що дозволяє забезпечити обмін даними без посередників та з високим рівнем впевненості у їхній легітимності.

Для забезпечення конфіденційності та анонімності в блокчейн-технологіях застосовуються різноманітні криптографічні методи та протоколи [2]. Асиметрична криптографія дозволяє використовувати пару ключів, яка включає в себе приватний та публічний ключ. На основі публічного ключа формується адреса акаунту, тоді як приватний ключ використовується для підпису транзакцій. Цей підхід дозволяє створювати безліч акаунтів навіть не комунікуючи з блокчейн-мережею.

Хоча блокчейн-мережі надають певний рівень конфіденційності, їх не можна вважати повністю анонімними, і у даній роботі аналізується вплив застосування логування на конфіденційність кінцевого користувача. Спершу розглядаються теоретичні аспекти, які коротко пояснюють мережеві протоколи та їх роль у блокчейн-мережах. Далі у роботі, формулюється завдання дослідження. Після цього аналізується застосування логування у різних учасниках блокчейн-мереж, а також умови та обмеження логування для деанонімізації кінцевого користувача.

Результати таких досліджень потрібні практиці, тому що вони дають розуміння конфіденційності у блокчейн-мережах, що сприяє більшої відкритості і, як наслідок, ширшому використанні та скорішому впровадженню блокчейн-технологій. Для користувачів це корисне, адже дає зрозуміти як їх взаємодія з різними учасниками мережі впливає на їх конфіденційність. Для криміналістів, що розслідують злочини пов'язані з крипто-діяльністю, результати таких досліджень важливі, адже надають додаткові інструменти для визначення кінцевого користувача у блокчейн-мережах [3].

Теоретичні аспекти

Зазвичай, будь-яка блокчейн-мережа використовує три типи мережевих протоколів для реалізації основного функціоналу [4, 5]: Node Discovery, Wire та JSON-RPC. Ці протоколи спільно керують складною мережевою взаємодією та комунікацій всередині блокчейн-екосистемах. Перший протокол, Node Discovery, сприяє ідентифікації та встановленню з’єднань між вузлами в мережі. Протокол Wire, другий у цій трійці, керує низькорівневою комунікацією між вузлами, визначаючи формат та структуру обмінюваних пакетів даних. А також третій, JSON-RPC протокол, який надає можливість виклику віддалених процедур по HTTP протоколу, дозволяючи користувачам та стороннім застосункам отримувати інформацію з блокчейн-мережі та надсилати інформацію до неї. Ця тріада протоколів спільно лежить в основі операційного фундаменту блокчейн-систем, організовуючи мережеву взаємодію.

Node Discovery – це зазвичай UDP протокол, що використовується в peer-to-peer мережах, таких як блокчейн-мережі, для автоматичного пошуку та з'єднання з іншими учасниками мережі. Основна мета протоколу Node Discovery полягає в тому, щоб забезпечити зручний та ефективний спосіб знаходження нових учасників і збереження списку вже відомих. У блокчейн-мережах зазвичай реалізується за допомогою алгоритму Kademlia [6]. Kademlia – це таблиця, в якій ключ являє собою логічну відстань між двома вузлами, а значення – набір вузлів, які знаходяться на даній відстані. Відстань є логічною, адже формується на основі ідентифікатора (публічного ключа) вузлів, а не мережевої адреси чи фізичного місця розташування.

Wire протокол – це TCP протокол, який використовується для обміну блокчейн-інформації, а саме, для синхронізації між вузлами, ретрансляції транзакцій і блоків та обміну іншими даними [7]. В Ethereum-подібних мережах побудований на RLPx-протоколі та забезпечує наскрізне шифрування між вузлами для конфіденційної передачі повідомлень.

JSON-RPC – високорівневий протокол побудований на HTTP. Протокол орієнтований не на взаємодію між вузлами, а на взаємодію між вузлом та клієнтом (користувачем або іншими застосунками). Для користувача є вхідною точною для взаємодії з блокчейн-мережею. JSON-RPC інтерфейс передбачає низку процедур, які дозволяють отримувати інформацію з мережі про транзакції, блоки, акаунти та надають можливість відправки інформації до блокчейну – підписаних транзакцій. Також може надавати процедури для управління вузлом.

Постановка завдання

Метою даного дослідження є визначення впливу процесу логування у різних типах учасників блокчейн-екосистеми на конфіденційність кінцевого користувача, а саме, на можливість його деанонімізації. Під деанонімізацією користувача розуміється отримання IP-адреси пристрою з якого було здійснено взаємодію з блокчейном. Хоча блокчейн-мережі вважаються конфіденційними, у даній роботі показано як логування, застосоване різними учасниками мережі впливає на конфіденційність відправника транзакції.

На практиці це дозволить встановити: для користувачів – на скільки взаємодія з учасниками мережі впливає на їх конфіденційність; для аналітиків – як логування може бути використане для деанонімізації кінцевого користувача.

Деанонімізація кінцевого користувача за допомогою логування

Хоча в блокчейн-мережах зазвичай усі вузли вважаються рівноправними, на практиці це не зовсім так. В залежності від типу учасника мережі логування може виконуватись на різних рівнях та мати різну ефективність. У даному розділі розглядається процес логування застосоване у різних типів учасників мережі та впливу на конфіденційність кінцевого користувача.

Логування на звичайних вузлах. Звичайні блокчейн-вузли є кістяком блокчейн-мереж (рис. 1). Вузли виконують завдання верифікації, яке полягає у впевненості в тому, що надіслані транзакції та блоки є правомірними та дотримуються встановлених протоколом правил. Після верифікації вузли ретранслюють транзакції та блоки до інших вузлів, а також додають ці блоки до локальної копії ланцюга блоків (повного або частково в залежності від типу вузла [8]). Це сприяє глобальному розповсюдженню та однорідності інформації, що забезпечує безпеку блокчейн-мереж.

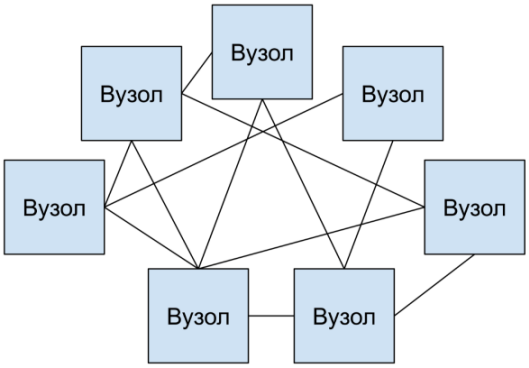

Рис. 1. Блокчейн-вузли формують мережу

Більшість вузлів працюють лише на низькорівневих протоколах Node Discovery і Wire, та не надають публічний JSON-RPC інтерфейс. При використанні низькорівневих протоколів, під час підключення іншого вузла до поточного або під час трансляції транзакції або блока з іншого вузла до поточного може здійснюватися логування, яке дозволить асоціювати IP-адресу вузла з трансльованою блокчейн-інформацією.

Обмеженням логування на персональному звичайному вузлі на рівні Wire протоколу є неможливість визначити чи вузол, який надіслав транзакцію, створив її сам або лише ретранслював транзакцію створену іншим вузлом. З іншого боку, якщо задача стоїть отримати всі транзакції ретрансльовані з вузла з певною IP-адресою, то підключившись до цього вузла ми почнемо отримувати транзакції та логувати їх.

Логування на публічних вузлах. Ще одним учасником мережі, якого можна виділити, є публічні вузли, які надаються зацікавленими сторонами для публічного використання. Треті особи, такі як розробники електронних гаманців, бірж та інших децентралізованих застосунків, розгортають і пропонують свої публічні сервери для користувачів. Якщо в документації блокчейн-мережі вказаний певний публічний вузол для загального використання, то зазвичай фактичним власником даного вузла є саме розробник даної мережі.

Публічні вузли надають JSON-RPC інтерфейс для Web-, мобільних застосунків та для розширень браузера для комунікації з мережею (рис. 2).

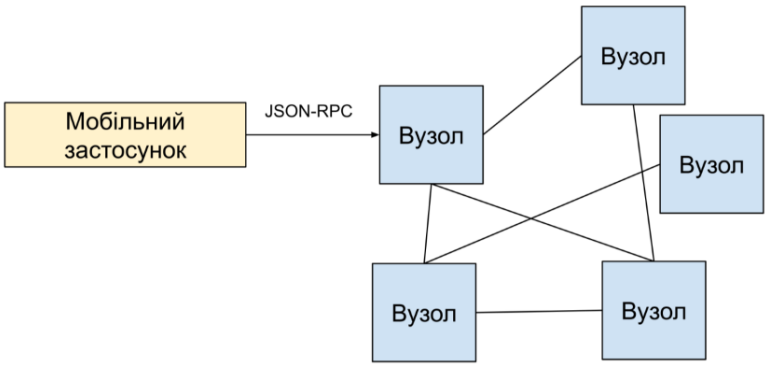

Рис. 2. Мобільний застосунок використовує JSON-RPC інтерфейс для комунікації з мережею

Застосунки у своїх налаштуваннях зазвичай за замовчуванням використовують певний публічний вузол. На рис. 3 показаний приклад налаштування електронного гаманця Metamask за замовчуванням.

Так як користувач напряму під'єднується до вузла через JSON-RPC протокол, то логування, застосоване на рівні даного протоколу дозволяє у більшості випадків ідентифікувати цього користувача. Наприклад, асоціювати виклик процедури відправки транзакції з IP-адресою пристрою, з якого було здійснене підключення до сервера.

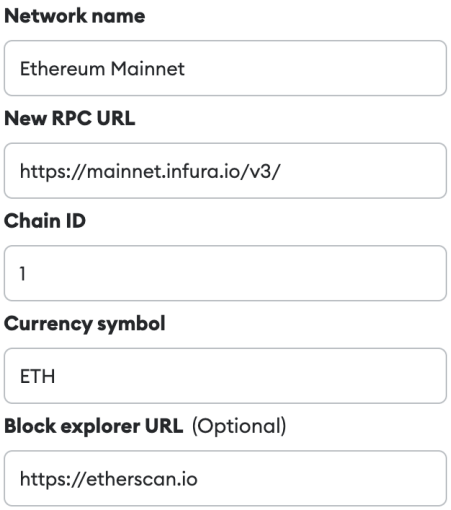

Рис. 3. Налаштування за замовчуванням для Ethereum мережі у електронному гаманці Metamask

Обмеженням даного методу є те, що застосунки за замовчуванням вказують публічний сервер, який має певну репутацію та довіру. Тому навіть, якщо розгорнути власний публічний сервер (або надати лише JSON-RPC інтерфейс), то навряд чи він буде застосований будь-яким децентралізованим додатком.

Логування на завантажувальних вузлах. Іншим особливим типом вузла є вузли завантаження (bootstrap/bootstrapping nodes). Вузол завантаження надає інформацію про конфігурацію мережі, в тому числі надає список вузлів до яких можливо здійснити підключення. Адреси вузлів завантажень прописані розробниками у налаштуваннях програмного забезпечення вузла, тому кожен новий клієнт мережі (вузол) спочатку підключається до вказаних вузлів завантаження, а вже потім до звичайних блокчейн-вузлів. В основному, вузли завантаження не реалізують основної логіки мережі, а слугують лише для надання списку вузлів, які несуть основну логіку. При підключенні до будь-якого вузла (в тому числі вузла завантаження), вузол який підключається, отримує список інших вузлів та додається до списку доступних. На рис. 4 блокчейн-вузол А здійснює підключення до завантажувальних вузлів для отримання списку інших вузлів мережі.

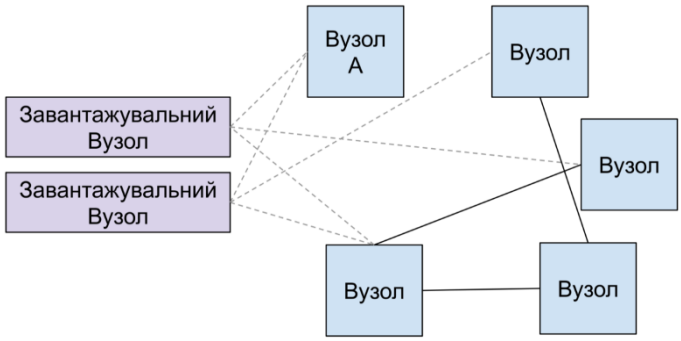

Рис. 4. Блокчейн-вузол А здійснює підключення до завантажувальних вузлів

Після отримання списку інших вузлів мережі, вузол А здійснює до них підключення (рис. 5).

Логування на завантажувальних серверах дозволяє отримати список усіх IP-адрес вузлів, що підключаються до мережі. Крім того, Node Discovery протокол передбачає використання ідентифікатора вузла (згенерований на основі його публічного ключа), який може бути асоційованим з IP-адресою вузла користувача.

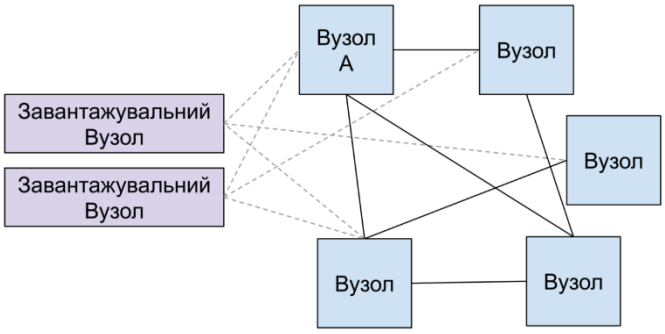

Рис. 5. Блокчейн-вузол А здійснює підключення до вузлів мережі

Завантажувальні вузли можуть бути розгорнуті будь-ким, але для того, щоб вони почали використовуватись як початкові вузли, вони повинні бути прописані у конфігураціях програмного забезпечення вузла. Для прикладу, у програмному забезпеченні вузлів Geth [9] за замовчуванням задані завантажувальні вузли [10], власниками яких є організація Ethereum Foundation [11].

Основним обмеженням застосування логування на завантажувальних серверах є те, що завантажувальні сервери суворо визначені у конфігураціях програмного забезпечення вузла, тому застосовувати даний метод можуть лише власники цих вузлів.

Ще одним обмеженням є те, що вузли завантаження не несуть основної логіки мережі і не обробляють транзакції. Тому не можна визначити з якого вузла, що підключався була відправлена транзакція, лише, що вузол з даною IP-адреса здійснив підключення до мережі і коли. Хоча це не може бути прямим методом ідентифікації кінцевого користувача, інформація про підключення до мережі і час підключення все ще може бути корисною в процесі аналізу. З іншого боку, якщо блокчейн-мережа досить мала, цієї інформації може бути достатньо для визначення IP-адреси користувача, який надіслав певну транзакцію.

Іншим недоліком даного методу є те, що він не гарантує, що вузол підключився до вузлів завантаження, які були вказані розробниками за замовчуванням. Користувач може самостійно вказати інші вузли для початкового підключення, тому до стандартних він може так і не підключитись.

Логування на майнінг-вузлах. Одним із особливих типів вузлів в Proof of Work (PoW) блокчейн-системах є майнінг-вузли (mining nodes). Ці вузли (рис. 6) не лише беруть на себе завдання приймати, верифікувати та ретранслювати транзакції, але й здійснюють процес генерації нових блоків за допомогою майнінг-процесу. Майнінг-вузли реалізують складний обчислювальний процес, який полягає у розв'язанні обчислювально-витратних криптографічних завдань, підтверджуючи легітимність транзакцій і формуючи новий блок, який включає в себе затверджені транзакції [12]. Після успішного процесу майнінгу блока, блок ретранслюється до інших блокчейн-вузлів, а майнінг-вузол отримує певну кількість криптовалюти, як винагороду за успішне виконання майнінг-процесу.

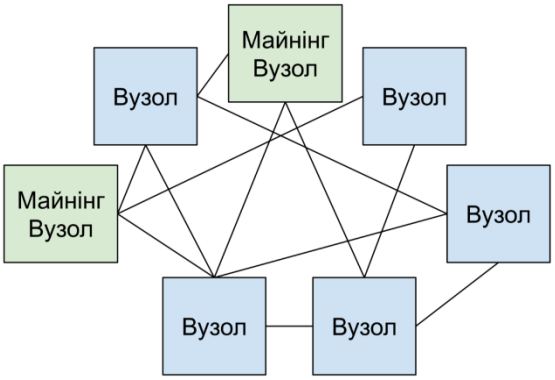

Рис. 6. Звичайні блокчейн-вузли та майнінг-вузли

Ці вузли використовують Node Discovery та Wire протоколи для комунікації з іншими вузлами. Також можуть мати активний JSON-RPC інтерфейс з додатковим функціоналом для управління процесом майнінгу [13].

Коли кінцевий користувач транслює створену транзакцію, вона ретранслюється іншими вузлами доки не досягне майнінг-вузлів. Але, кінцевий користувач може уникати проміжних вузлів та надсилати транзакцію напряму майнінг-вузлам, за умови, що він знає їхні адреси та не має обмежень на боці майнінг-вузлів. Це дозволяє уникнути аналізу та збору інформації про транзакцію користувача проміжними вузлами [14]. Таким чином, у разі прямого з'єднання, майнінг-вузол має можливість зв'язати транзакцію користувача з його IP-адресою.

Власниками майнінг вузлів можуть бути як приватні особи, так і великі корпорації. Немає обмежень на розгортання майнінг-вузлів і будь-хто може розгорнути майнінг вузол з невеликими ресурсами задля потенційного логування користувачів.

Основним обмеженням застосування логування на майнінг-вузлах задля ідентифікації кінцевого користувача є те, що клієнт повинен відправити транзакцію напряму до майнінг-вузла. В іншому випадку, логування на майнінг-вузлі невиправдане, адже транзакцію буде ретрансльовано проміжним вузлом і виникає така ж проблема як і при логування на звичайних вузлах.

Логування у блокчейн експлорерах. Іншим учасником блокчейн екосистем є блокчейн експлорери (blockchain explorers), які надаються більшістю блокчейн-мереж для своїх користувачів. Хоча блокчейн експлорери не є напряму елементами саме блокчейн-мереж, вони є важливим інструментом для її дослідження. Блокчейн експлорер – це інструмент, зазвичай реалізований у вигляді веб-застосунку, який дозволяє користувачам проводити аналіз та дослідження даних у блокчейн-мережі, зокрема транзакцій, гаманців, блоків тощо. Він надає можливість детального вивчення та візуалізації даних, наприклад, для перевірки чи успішно була виконана транзакція користувача. На рис. 7 зображена головна сторінка блокчейн експлорера Etherscan для мережі Ethereum. Користувач зазвичай використовує блокчейн експлорер

для перевірки балансу його аккаунту, або для пошуку відправленої транзакції та перевірки чи була вона включена у блокчейн.

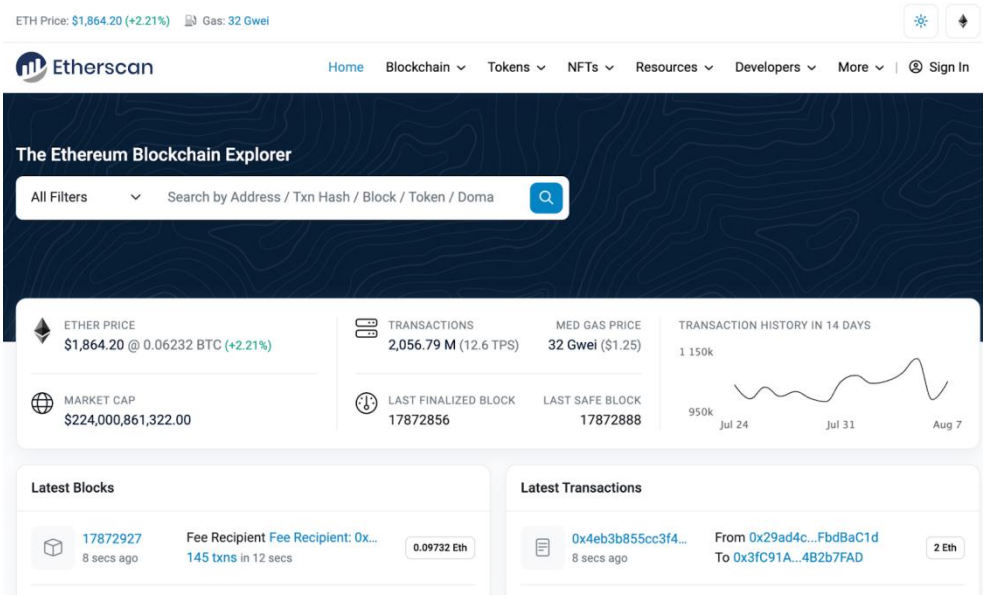

Рис. 7. Головна сторінка Etherscan

Логування взаємодії користувача з блокчейн експлорером на рівні HTTP протоколу дозволяє достатньо точно встановити зв'язок IP-адреси користувача з інформацією, яку він запитував. Наприклад, якщо користувач запитує певну транзакцію, то це дозволяє асоціювати його IP-адресу з цією транзакцією, з відправником транзакції або отримувачем транзакції. Крім того, використання браузера для доступу до блокчейн експлорера збільшує ризики деанонімізації користувача навіть у випадках використання VPN чи TOR [15] [16] [17].

Власниками блокчейн експлорерів зазвичай є розробники блокчейн-мережі, приватні компанії та приватні особи [18]. Немає обмежень на розгортання власного блокчейн експлорера, але для того, щоб їм почали активно користуватись і можливо було отримувати результати з ідентифікації користувачів, потрібні зусилля з його популяризації. Це і є основним обмеженням.

Іншим обмеженням є те, що зв'язок IP-адреси з певною транзакцією чи аккаунтом не гарантує, що саме цей користувач є його власником або відправником транзакції. Хоча це може спонукати на подальший аналіз цього зв'язка, наприклад визначити, чому даний користувач здійснив пошук у блокчейн експлорері саме цієї транзакції.

Висновки

У даній роботі проаналізовані різні учасники блокчейн-екосистем, та як ці учасники можуть використовувати процес логування для деанонімізації кінцевого користувача. Серед учасників мережі було виокремлено завантажувальні вузли, публічні вузли, звичайні вузли, майнінг-вузли та блокчейн експлорери.

Проведений аналіз дозволяє стверджувати, що логування може бути ефективним способом для деанонімізації кінцевого користувача та є серйозним викликом для його конфіденційності.

Також, проаналізовано, що логування має певні обмеження. Загальним і основним обмеженням є те, що кінцевий користувач повинен напряму здійснити підключення до учасника мережі, який намагається асоціювати IP-адресу пристрою користувача з даними, які він надсилає.

Подальшим етапом наукового дослідження може стати осмислення перспектив та формулювання стратегій, спрямованих на подолання обмежень, що описані у даній роботі. Найбільш практичним напрямком може бути спонукання кінцевого користувач здійснити підключення до учасника мережі, що намагається його ідентифікувати, а саме асоціювати IP-адресу з даними, які надсилаються або отримуються з блокчейн-мережі.

References

1. Cachin, C., & Vukolić, M. (2017). Blockchain Consensus Protocols in the Wild (Version 2). arXiv. https://doi.org/10.48550/ARXIV.1707.01873

2. Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain (Version 2). arXiv. https://doi.org/10.48550/ARXIV.1903.07602

3. Dorogyy, Y., Kolisnichenko, V. (in press). Blockchain Transaction Analysis: A Comprehensive Review of Applications, Tasks and Methods. System research and information technologies.

4. Dotan, M., Pignolet, Y.-A., Schmid, S., Tochner, S., & Zohar, A. (2020). Survey on Cryptocurrency Networking: Context, State-of-the-Art, Challenges (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2008.08412

5. Luo, Z., Murukutla, R., & Kate, A. (2022). Last Mile of Blockchains: RPC and Node-as-a-service (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2212.03383

6. Hassanzadeh-Nazarabadi, Y., Taheri-Boshrooyeh, S., Otoum, S., Ucar, S., & Özkasap, Ö. (2021). DHT-based Communications Survey: Architectures and Use Cases (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2109.10787

7. Wang, T., Zhao, C., Yang, Q., Zhang, S., & Liew, S. C. (2020). Ethna: Analyzing the Underlying Peer-to-Peer Network of the Ethereum Blockchain (Version 2). arXiv. https://doi.org/10.48550/ARXIV.2010.01373

8. Sync modes. (n.d.). Retrieved August 15, 2023. https://geth.ethereum.org/docs/fundamentals/sync-modes

9. go-ethereum. (n.d.). Retrieved August 15, 2023. https://geth.ethereum.org

10. go-ethereum/params/bootnodes.go. (n.d.). Retrieved August 15, 2023. https://github.com/ethereum/go-ethereum/blob/67979022aa8ea6a96b618c086f60b49af7d2a568/params/bootnodes.go#L23

11. Ethereum Foundation. (n.d.). Retrieved August 15, 2023. https://ethereum.org/en/foundation/

12. Grunspan, C., & Pérez-Marco, R. (2020). The mathematics of Bitcoin. arXiv. https://doi.org/10.48550/ARXIV.2003.00001

13. Miner namespace. (n.d.). Retrieved August 15, 2023. https://geth.ethereum.org/docs/interacting-with-geth/rpc/ns-miner

14. How to send private transactions on ethereum. (n.d.). Retrieved August 15, 2023. https://www.alchemy.com/overviews/ethereum-private-transactions

15. Al-Fannah, N. M. (2017). One leak will sink a ship: WebRTC IP address leaks. In 2017 International Carnahan Conference on Security Technology (ICCST). 2017 International Carnahan Conference on Security Technology (ICCST). IEEE. https://doi.org/10.1109/ccst.2017.8167801

16. Lu, Y., & Tsudik, G. (2010). Towards Plugging Privacy Leaks in the Domain Name System. In 2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P). 2010 IEEE Tenth International Conference on Peer-to-Peer Computing (P2P). IEEE. https://doi.org/10.1109/p2p.2010.5569976

17. Browserleaks - Check your browser for privacy leaks. (n.d.). Retrieved August 15, 2023. https://browserleaks.com/

18. Etherscan - Crunchbase Company Profile. (n.d.). Retrieved August 15, 2023. https://www.crunchbase.com/organization/etherscan