УДК 004.56
А. Кобельник; І. Скарга-Бандурова, д. т. н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ІНСТРУМЕНТУ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ДІЙ В БЛОКЧЕЙНІ

UDC 004.56
A. Kobelnyk; I. Skarga-Bandurova, Doctor of Technical Sciences, Prof.

DEVELOPMENT OF A BLOCKCHAIN FRAUD DETECTION TOOL

Розвиток блокчейну за останні кілька років перетворив його з нішевої технології на глобальну інфраструктуру вартістю понад 3,2 трлн доларів [1], але водночас створив ідеальне середовище для наймасштабнішого в історії перерозподілу капіталу через шахрайство. Децентралізація, прозорість та незмінність даних у блокчейн-середовищах забезпечують нові можливості для користувачів, проте одночасно створюють сприятливі умови для появи складних, автоматизованих форм шахрайства. Масштабність і відкритість Web3 призводять до того, що виявлення ризиків і відокремлення легітимної активності від шахрайської стає технічно складним завданням.

Провідні аналітичні платформи, такі як Chainalysis [2], Elliptic [3], TRM Labs [4], що спеціалізуються на криптобезпеці та AML-комплаєнсі, пропонують моніторинг транзакцій та криміналістичну експертизу. Однак, їхні послуги орієнтовані насамперед на великі фінансові установи та правоохоронні органи, вимагаючи значних фінансових ресурсів і доступу до закритих корпоративних інтерфейсів. Це залишає звичайний користувачів практично без інструментів для самостійного аналізу даних.

З огляду на це, актуальним стає створення доступного інструменту, який дозволяє кожному користувачеві самостійно оцінювати безпеку взаємодії з EVM-адресами. Він вирішує кілька ключових завдань: збір і систематизацію відкритих ончейн-даних, наочну візуалізацію транзакційних взаємодій, проведення розслідувань та формування зрозумілої оцінки ризику.

Інструмент використовує дані з відкритих джерел і безкоштовних API, що робить його доступним для широкого кола користувачів і незалежним від дорогих корпоративних рішень. Отримані дані відображаються у вигляді графів, що дозволяє швидко оцінити структуру зв’язків між адресами та помітити потенційно підозрілу активність. Оцінка ризику здійснюється автоматично або інтерактивно у вигляді анкети, що забезпечує працездатність навіть при обмеженому доступі до потрібних даних через API. Такий підхід не лише зберігає функціональність системи, а й перетворює процес аналізу на навчальний досвід: користувач освоює принципи розпізнавання шахрайської активності та може застосовувати ці знання в майбутньому. Проведене тестування на реальних випадках показало, що інструмент демонструє високу точність оцінки ризику та надійно ідентифікує підозрілу активність у різних сценаріях.

Перспективи розвитку охоплюють підтримку non-EVM блкочейнів, вдосконалення методів аналітики та взаємодій через кросчейн мости, розширення оцінки різних видів шахрайства та впровадження модуля для аналізу смарт-контрактів, що дозволить виявляти потенційно небезпечну логіку всередині контрактів. Додатково розглядається створення бази знань, що сприятиме формуванню в користувачів практичних навичок оцінювання ризиків і загальної цифрової безпеки, адже усвідомлене розуміння механізмів шахрайства та принципів безпечної поведінки суттєво знижує ймовірність фінансових втрат.

Література

1. Cryptocu Global Cryptocurrency Market Cap Charts. CoinGecko. URL: https://www.coingecko.com/en/charts.
2. The Blockchain Data Platform. Chainalysis. URL: https://www.chainalysis.com/.
3. Elliptic: Blockchain Analytics & Crypto Compliance Solutions. Elliptic. URL: https://www.elliptic.co/.
4. TRM Labs | Blockchain Intelligence Platform. TRM Labs. URL: https://www.trmlabs.com/.