УДК 343.1:65.012.8+004 DOI: https://doi.org/10.32631/pb.2021.1.13

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ,
кандидат технічних наук, доцент,
Харківський національний університет внутрішніх справ;
https://orcid.org/0000-0002-7848-6448,
e-mail: vitnos.g@gmail.com;

ІРИНА АНДРІЇВНА МАНЖАЙ,
ТОВ «Харківський університет»;
https://orcid.org/0000-0003-2664-4472,
e-mail: irinamanzhai@gmail.com

ОКРЕМІ АСПЕКТИ АНАЛІЗУ КРИПТОВАЛЮТНИХ ТРАНСАКЦІЙ ПІД ЧАС ПОПЕРЕДЖЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

Проведено аналіз окремих інструментів для візуалізації руху криптовалютних цінностей, а також ідентифікації користувачів, які здійснили відповідні трансакції. Вивчено переваги та недоліки криптовалюти з точки зору правопорушників та правоохоронних органів. Визначено головні напрямки використання криптовалют у злочинному середовищі. Проаналізовано поточний стан та перспективи нормативно-правового регулювання криптовалют в Україні. Вивчено теоретичні засади функціонування криптовалют. Розкрито можливості окремих сервісів, призначених для аналізу криптовалютних трансакцій. На прикладі роботи сервісу «Crystal Expert» продемонстровано процес оцінки ризиків та побудови візуальних ланцюжків криптовалютних трансакцій. На підставі проведеного аналізу визначено основні завдання для правоохоронних органів на нинішньому етапі розвитку криптовалют.

Ключові слова: *криптовалюта, аналіз трансакцій, візуалізація, правоохоронні органи, протидія злочинності*

Оригінальна стаття

Постановка проблеми

Минуло вже більше десяти років із часу створення перших криптовалют. За цей час ця категорія активів отримала достатньо широке визнання у всьому світі як серед законослухняних громадян, так і серед правопорушників. Головними перевагами криптовалюти, які є особливо привабливими для зловмисників, можна назвати складність відслідковування власника подібних цінностей, фактичну неможливість контролю над проведенням відповідних операцій з криптовалютою з боку державних органів, транскордонність, що дозволяє оперувати значними коштами без сплати відповідних митних платежів. Подібні причини зазначають і американські науковці [1, с. 334].

Сьогодні в українському сегменті «злочинного бізнесу» криптовалюти використовуються, як правило, для оплати в сумнівних оборудках та відмивання коштів, одержаних злочинним шляхом. Значна частина таких трансакцій відбувається в рамках роботи Інтернет-наркокрамниць та у процесі вимагання. Подібні тенденції є характерними й для інших країн, що підтверджується відповідними дослідженнями [2; 3; 4; 5]. Великих збитків може також завдати створення фінансових пірамід, пов'язаних із випуском нових криптовалют [6].

Певна складність у проведенні операцій з криптовалютами, їх волатильність та високі комісії в цій сфері на нинішньому етапі розвитку заважають широкому впровадженню цієї технології як універсального способу оплати у злочинних схемах. Спостерігається тенденція до збільшення використання криптовалют саме для відмивання коштів, одержаних злочинним шляхом. Як слушно зазначають окремі автори [7, с. 213], криптовалюти є потенційно небезпечними з точки зору дестабілізаційного впливу на фіатну валюту і втрати контролю державними органами над розвитком економіки. До того ж досить складно проводити розслідування злочинів із криптовалютами через їх децентралізований характер.

Ураховуючи викладене, для правоохоронних органів усього світу стає вкрай актуальним розроблення дієвого механізму ідентифікації осіб, яким належать відповідні криптовалютні активи, а також представлення руху таких коштів у зрозумілому вигляді для осіб, які здійснюють попередження та розслідування злочинів.

Стан дослідження проблеми

Дослідженням проблем протидії використанню криптовалют у злочинних схемах присвячено роботи таких авторів, як І. Алєксєєнко, Т. Герелюк, Ю. Дорохіна, О. Дроздов, О. Дроздова, А. Ковальчук, В. Козій, С. Леськів, Л. Омельчук, І. Патерило Д. Пашко, А. Проценко, С. Стеценко, К. Чижмарь, С. Шевченко, О. Юнін та ін. Разом із тим украй незначною є кількість праць, де висвітлено саме аналіз трансакцій із криптовалютами в контексті виконання завдань протидії злочинності. Що стосується україномовних наукових джерел, то нам не вдалося знайти жодної статті, присвяченої висвітленню особливостей аналізу трансакцій криптовалют для виконання завдань протидії злочинності.

Мета і завдання дослідження.

Метою статті є проведення аналізу окремих інструментів для візуалізації руху криптовалютних цінностей, а також ідентифікації користувачів, які здійснили відповідні трансакції. Для досягнення цієї мети потрібно виконати такі *завдання*:

– вивчити виклики для правоохоронних органів, пов'язані з функціонуванням криптовалютних систем;

– визначити теоретичні засади функціонування криптовалют;

– проаналізувати головні програмні інструменти для аналізу криптовалютних трансакцій.

Наукова новизна дослідження

Робота є однією з перших спроб аналізу існуючих інструментів аналізу криптовалютних трансакцій для виконання завдань українських правоохоронних органів.

Виклад основного матеріалу

В українському законодавстві питання обігу криптовалют усе ще залишається недостатньо врегульованим. Свого часу до Верховної Ради України було подано низку законопроєктів, покликаних певною мірою врегулювати ринок криптовалют на території України, проте вони не набули статусу законів[1], а були відкликані. 2 грудня 2020 р. Верховна Рада України у першому читанні ухвалила законопроєкт «Про віртуальні активи»[2], згідно з яким криптовалюта може розглядатися як різновид віртуальних активів – особливого виду майна, який є цінністю в електронній формі, існує в системі обігу віртуальних активів та може знаходитись у цивільному обігу. Втім, досі невідомо, коли згаданий законопроєкт зможе набути статусу закону та чи взагалі це відбудеться. Враховуючи викладене, сьогодні під час роботи з криптовалютами підприємці та правоохоронні органи користуються загальними нормами законодавства, які не враховують специфіку таких цінностей. Однією з гострих проблем у цьому контексті є питання накладання арешту на подібні активи, який практично неможливо здійснити за нормами чинного Кримінального процесуального кодексу.

Перед тим, як перейти до питання аналізу трансакцій з криптовалютами, слід коротко розглянути теоретичні засади їх функціонування.

Перш за все слід зазначити, що криптовалюти оперують деякими цінностями, а не реальними валютами. По суті, вони є віртуальною готівкою, а не зобов'язанням емітента видати реальну валюту або оплатити товар онлайн. Також криптовалюти не мають єдиного емітента – всі учасники системи за певним протоколом емітують нові цінності.

Псевдоанонімність роботи з криптовалютами забезпечується з використанням асиметричної криптографії та однорангової мережі (P2P) без необхідності залучення довіреної третьої сторони [8, с. 9].

Для збереження інформації про всі трансакції з криптовалютами використовується спеціальна розподілена база даних – блокчейн

[1] Проект Закону про обіг криптовалюти в Україні : від 06.10.2017 № 7183 / ініціатори І. О. Котвіцький, І. П. Рибак, С. М. Войцеховська // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684 (дата звернення: 13.12.2020); Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні : від 10.10.2017 № 7183-1 / ініціатор С. В. Рибалка // БД «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710 (дата звернення: 13.12.2020); Проект Закону про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні) : від 30.10.2017 № 7246 / ініціатор С. В. Рибалка // БД «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62816 (дата звернення: 13.12.2020).

[2] Проект Закону про віртуальні активи : від 11.06.2020 № 3637 / ініціатори О. С. Жмеренецький, М. Р. Потураєв, І. С. Васильєв та ін. // БД «Законодавство України» / ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110 (дата звернення: 13.12.2020).

(*blockchain*). У цій базі даних зберігаються обмежені відомості про трансакції, та вони не дають можливості правоохоронним органам безпосередньо дізнатися, хто саме здійснював відповідні операції.

Крім певних ускладнень, що пов'язані з ідентифікацією осіб, які здійснювали ті чи інші трансакції з використанням криптовалют, технологія блокчейн має також низку позитивних особливостей, корисних для виконання завдань протидії злочинності. Передусім це фіксація всіх операцій від початку і до кінця в системі. Їх неможливо видалити або виправити. Таким чином, правоохоронні органи можуть зібрати всю інформацію про відповідні операції. Крім того, важливою перевагою для правоохоронців є фіксація часу проведення певних трансакцій. Особливо проблемним моментом для правоохоронних органів може стати використання правопорушниками кількох видів криптовалют у ланцюжку протиправних операцій [9].

Однією з перших та найбільш відомих криптовалют є біткоїн. У платіжній системі біткоїн децентралізовано емісію монет, підтвердження трансакцій, зберігання даних, аудит облікової системи, прийняття рішення щодо оновлень протоколів і програмного забезпечення.

Під час розслідування кримінальних правопорушень, де фігурують криптовалюти, зокрема біткоїн, вхідною для аналізу є біткоїн-адреса – ідентифікатор, із яким у розподіленій базі даних асоційований певний баланс біткоїн-монет. Біткоїн-адреси можуть бути представлені у двох форматах – Base58 і Bech32.

Для витрачання коштів із біткоїн-адреси (формування трансакції) залежно від типу адреси потрібно знати один або декілька приватних (секретних) ключів. Адресі, що починається з цифри 1, відповідає один приватний (секретний) ключ, знання якого дозволяє підписувати трансакцію при витрачанні коштів із цієї адреси. Адресі, що починається з цифри 3, поставлено у відповідність декілька приватних ключів. У цьому випадку залежно від визначеного сценарію для підпису трансакції потрібно використати або всі, або певну кількість ключів з усіх.

Адреса є анонімною і не містить інформації про власника. Генерація адреси здійснюється відповідним програмним забезпеченням локально без підключення до мережі біткоїн.

Одна людина може мати необмежену кількість біткоїн-адрес. Кожного разу для отримання коштів можна створювати нову адресу. Програмне забезпечення біткоїн-гаманця може оперувати будь-якою кількістю адрес, або кожна адреса може обслуговуватися окремим гаманцем.

Усі затверджені трансакції (ті, що потрапили у блокчейн) у вигляді блоків із зазначенням суми, адреси-відправника й адреси-отримувача знаходяться у вільному доступі та доступні для ознайомлення на різноманітних ресурсах Інтернету. Будь-який користувач може завантажити увесь актуальний журнал біткоїн-трансакцій (блокчейн), що надає принципову можливість побудувати ланцюг руху коштів між різними біткоїн-адресами.

На рис. 1 показана структура однієї з трансакцій.

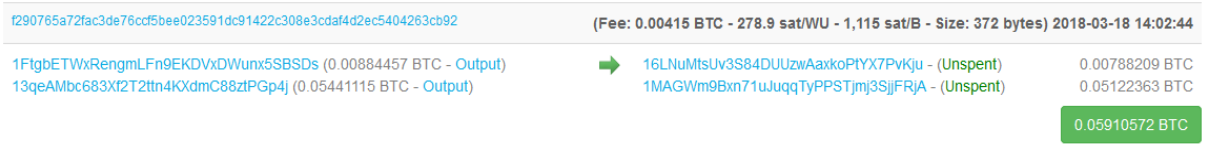

Рис. 1. Структура біткоїн-трансакції

Отже, на рис. 1 можна побачити унікальний номер трансакції:

f290765a72fac3de76ccf5bee023591dc91422c308e3cdaf4d2ec5404263cb92.

Імовірно, одна особа (якщо не застосовувались засоби додаткової анонімізації) володіє двома рахунками з відповідними балансами:

1FtgbETWxRengmLFn9EKDVxDWunx5SBSDs (0.00884457 BTC),

13qeAMbc683Xf2T2ttn4KXdmC88ztPGp4j (0.05441115 BTC),

оскільки ініціює одночасно два перекази на дві адреси, з яких монети ще не витрачені:

16LNuMtsUv3S84DUUzwAaxkoPtYX7PvKju - (Unspent) 0.00788209 BTC,

1MAGWm9Bxn71uJuqqTyPPSTjmj3SjjFRjA - (Unspent) 0.05122363 BTC.

Імовірно, одна з адрес отримання належить ініціатору трансакції, куди він перераховує остачу. Таким чином, можна відслідкувати ланцюг руху коштів із виходу з певної адреси до входу на іншу (інші).

Із метою ускладнення аналізу біткоїн-трансакцій у глобальній мережі з'явилися ресурси, що пропонують послуги «мікшування» шляхом прийняття спочатку на одну адресу

або кілька адрес коштів від багатьох користувачів, а потім у випадковому порядку і з різною затримкою в різних трансакціях переказ коштів на адреси, що наперед визначені користувачами сервісу мікшування. Також існує метод підвищення анонімності CoinJoin, який не потребує наявності третьої довіреної сторони, а передбачає об'єднання переказів в одну трансакцію від декількох користувачів.

Наявні біткоїн-адреси за допомогою пошукових сервісів потенційно можливо зв'язати із IP-адресою, доменним ім'ям, електронною поштою, обліковим записом користувача якого-небудь сервісу, ідентифікатором соціальних мереж тощо. Анонімність біткоїн-адреси втрачається під час обміну монет біткоїн на фіатну (звичайну) валюту в обмінних сервісах, біржах тощо.

Як засіб автоматизації пошуку та побудови схеми відношень різних ідентифікаторів біткоїн-трансакцій можна використовувати безкоштовну програму Maltego Community Edition (maltego.com) зі встановленим трансформатором аналізу біткоїн-ідентифікаторів. Приклад побудови логічної схеми трансакцій між певними адресами наведений на рис. 2.

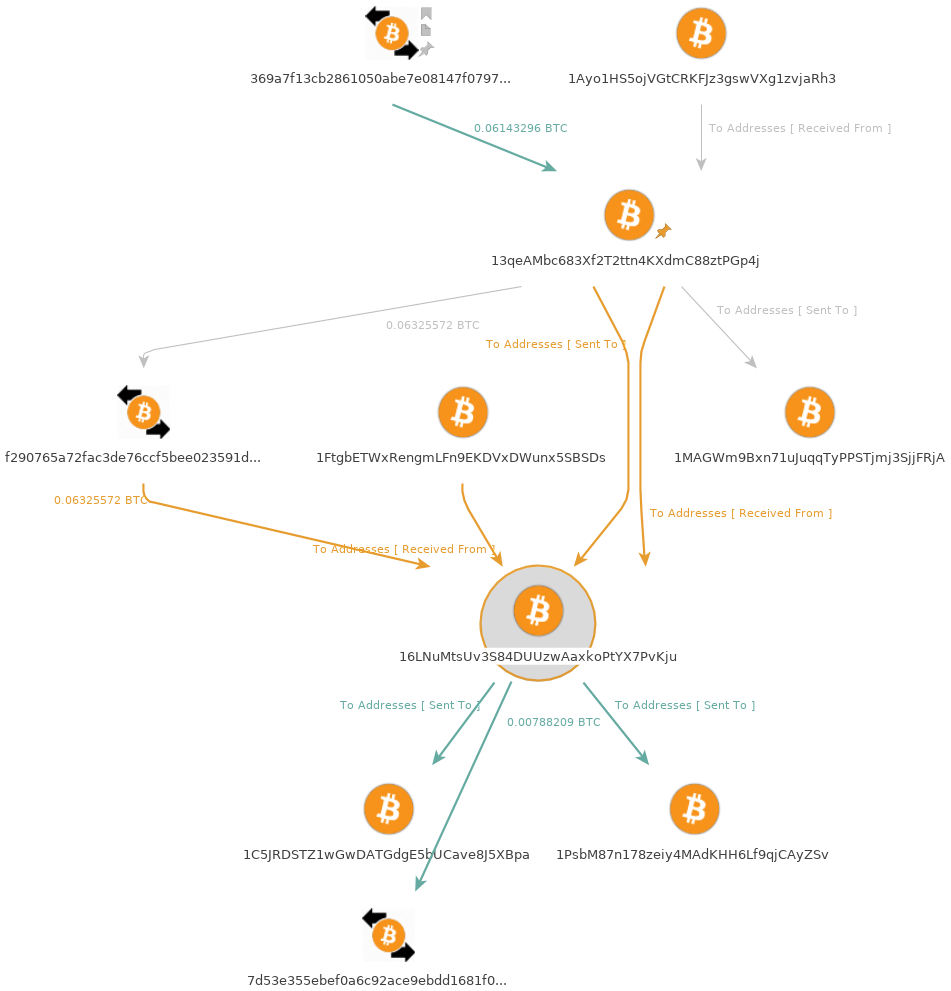

Рис. 2. Приклад побудови логічної схеми трансакцій між певними адресами в Maltego Community Edition

Проведений аналіз засвідчив, що серед інструментів аналізу в роботі правоохоронних органів також можна застосовувати:

– bitconeview.info – для візуалізації трансакцій;

– github.com/mikispag/bitiodine – для аналізу біткоїн блокчейн із можливістю кластеризації;

– github.com/BitcoinOpReturn/OpReturnTool – для вилучення OP_RETURN метаданих з біткоїн блокчейн;

– blockchain.info – для швидкого виконання базових функцій аналізу трансакцій;

– anyblockanalytics.com – для аналізу руху різних криптовалют;

– Chainalysis, Elliptic, Ciphertrace, Blockchain Inspector – для аналізу ризиків, пов'язаних із біткоїн-трансакціями.

Одним із потужних інструментів аналізу є платформа crystalblockchain.com, яка дозволяє проводити ризик-аналіз Bitcoin (BTC), Bitcoin Cash (BCH), Ethereum (ETH), Ethereum tokens: ERC20 & ERC721, Litecoin (LTC), Tether (USDT), Ripple (XRP).

Основною аналітичною цінністю сервісу «Crystal Expert» є база ідентифікованих та неідентифікованих володільців (*entities*) біткоїн-адрес, що підтримується в актуальному стані. На момент написання роботи база містила 3299 володільців біткоїн-адрес (*Bitcoin Entities*), які розділені на такі типи: автомати покупки/продажу біткоїн; кримінальні торгові майданчики в TOR мережі; суб'єкти надання нелегальних послуг за криптовалюту через TOR мережу; криптовалютні біржі з градацією ризику відмивання грошей; шахрайські обмінники криптовалют; сайти азартних ігор; нелегальні сервіси з оплатою криптовалютою; майнери криптовалют; сервіси мікшування; легальні онлайн-сервіси надання послуг, пов'язаних із криптовалютою; сервіси онлайн-гаманців; некласифіковані сервіси, що пов'язані з криптовалютою; системи обробки криптовалютних платежів; програми – вимагачі криптовалют; шахрайські ресурси, пов'язані з криптовалютами; адреси, на які виводились вкрадені монети.

Кожному типу володільця (*entity type*) або володільцю біткоїн-адрес (*entity*) призначається або розраховується оцінка ризику (*Risk Score*) на підставі імовірної участі у протиправній діяльності та легальності походження коштів. Налаштування власного профілю шкали оцінки ризику дозволяє враховувати особливості розслідування.

Наприклад, для визначеного на рис. 3 профілю шкали оцінки ризику величина ризику неідентифікованих володільців біткоїн-адрес (*Unnamed Entity*), які отримують і відправляють кошти через проміжні біткоїн-адреси, показана на рис. 4. Зміна профілю шкали оцінки ризику призводить до зміни величини ризику для тих же неідентифікованих володільців біткоїн-адрес.

Entity type	Risk Score	Receiving direction	Sending direction
Darknet Marketplace	100%	None	High
Exchange With High ML Risk	25%	High	None
Gambling	75%	High	High
Ransom	50%	High	High

Рис. 3. Тестовий профіль № 1 шкали оцінки ризику

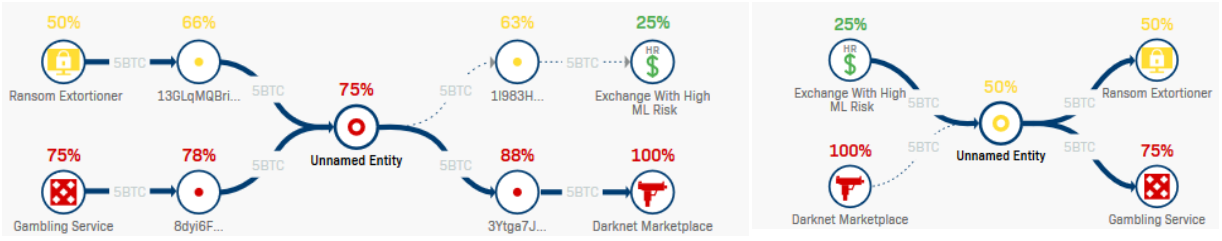

Рис. 4. Обчислений згідно з тестовим профілем № 1 ризик неідентифікованих володільців біткоїн-адрес

«Crystal Expert» містить 5 основних і 2 додаткових інструменти розслідування.

Інструмент «Справи (*Cases*)» призначено для управління розслідуваннями у вигляді справ. Тут можна створювати нові справи і переглядати поточні. Сторінка справи містить основні деталі, адреси, візуалізації та відстеження, додані до справи.

Інструмент «Дослідник (*Explorer*)» призначений для дослідження трансакцій, блоків та адрес, а також відображення інформації про ідентифікованих володільців біткоїн-адрес, їх типи, основні майнери та курс біткоїна.

Інструмент «Відстеження (*Tracking*)» дозволяє відстежувати у часі подальший рух коштів за визначеною трансакцією або групою

трансакцій. Відстеження може виявити, чи потрапили вихідні кошти з певної трансакції до ідентифікованого володільця біткоїн-адрес, наприклад біржі або платіжного процесора, що, у свою чергу, може дозволити ідентифікувати через відповідні правові процедури власника вихідної біткоїн-адреси.

Інструмент «Монітор (*Monitor*)» в основному призначений для compliance-офіцерів фінансових інституцій, дозволяє за налаштованими правилами перевіряти ступінь ризикованості (*Risk Score*) певних трансакцій.

Інструмент «Інформаційна панель (*Dashboard*)» розділений на секції інформування користувача про створені і збережені ним: справи, візуалізації, переліки відстеження руху коштів, закладки сторінок аналізу адрес, блоків трансакцій, трансакцій та володільців адрес.

Під час дослідження в основному інструменті «Дослідник» певної біткоїн-адреси Crystal надає інформацію про категорію володільця адреси, поточний баланс, кількість трансакцій, поточний стан, дати першої і останньої активності, величину ризику (*Risk Score*) щодо імовірної участі у кримінальній діяльності і кримінальності походження коштів.

Тут же для володільця цієї адреси відображається загальна якісно-кількісна діаграма взаємодії (отримання і відправлення коштів) з іншими ідентифікованими володільцями біткоїн-адрес із зазначенням величини ризику (рис. 5).

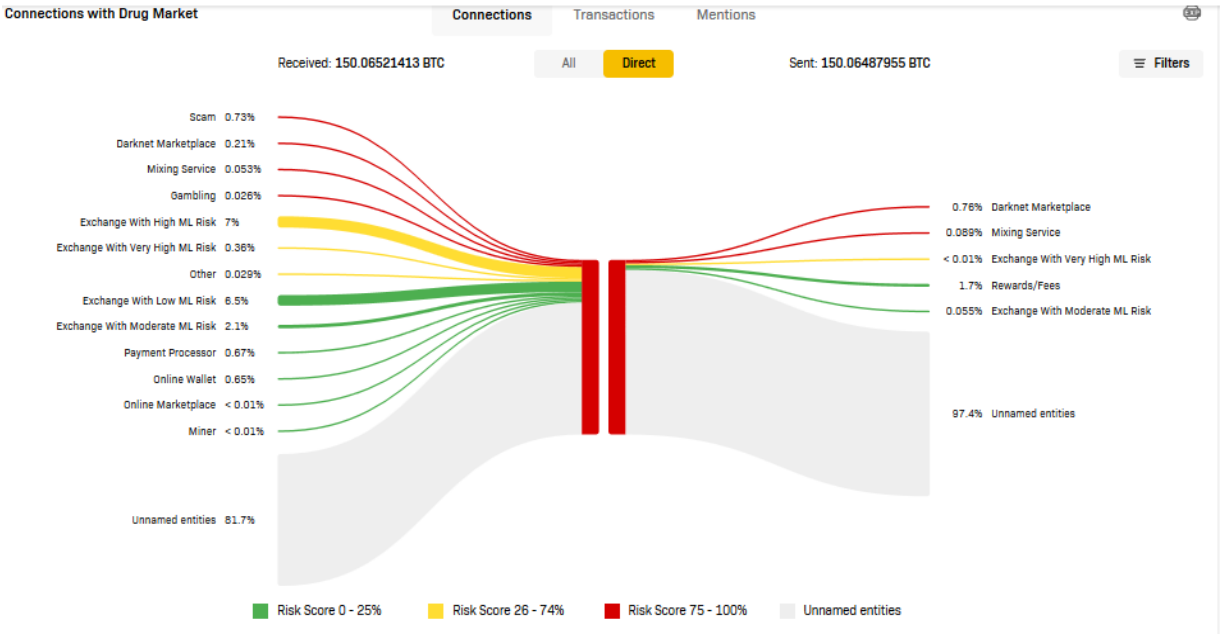

Рис. 5. Якісно-кількісна діаграма взаємодії (отримання і відправлення коштів) володільця певної біткоїн-адреси з іншими ідентифікованими володільцями біткоїн-адрес

Через інструмент «Візуалізація (*Visualization*)» трансакції з досліджуваною біткоїн-адресою можна зобразити у вигляді графа (рис. 6) та керувати відображенням його вузлів.

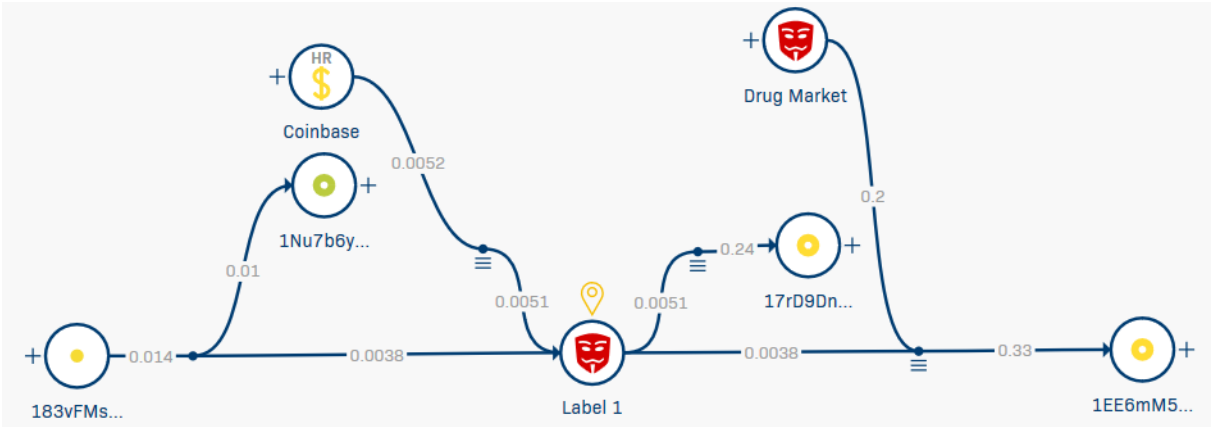

Рис. 6. Візуалізація трансакцій з досліджуваною біткоїн-адресою

З огляду на зазначений функціонал платформа «Crystal Expert» може ефективно забезпечувати розслідування кримінальних правопорушень, у яких фігурують визначені криптовалюти.

Висновки

Описані в цій роботі виклики, які породжує впровадження криптовалют, не є вичерпними. Очевидно, що існує багато інших особливостей функціонування цієї категорії цінностей, які поки що не потрапляють у поле зору вітчизняних та зарубіжних правоохоронних органів. Одним із таких викликів є розміщення в системі блокчейн забороненого контенту, який практично неможливо буде прибрати через особливості функціонування платформи. Як інструмент для демонстрації такого контенту можна згадати проєкт cryptograffiti.info, який допомагає завантажувати із системи блокчейн наявні там зображення. Будь-хто при цьому під час формування трансакцій може завантажити свій контент, як приватні фотознімки (cryptograffiti.info/cache/4e45e78eabc567e004f71cf36f23c7ab814cc96c, cryptograffiti.info/cache/53f3c728dbe12490ccd0a7c8c4b18f26f1dd75e7), так і більш сумнівні дані (cryptograffiti.info/cache/d9fd30e79bbf33adedd0edd4b5133d7f96c2bd00). На прикладі іншого подібного проєкту (github.com/zyk11) мальтійські вчені свого часу досить переконливо обґрунтували існування загрози розміщення подібним чином у системі блокчейн дитячої порнографії [10].

Ураховуючи викладене, можна сформулювати низку головних завдань для правоохоронних органів на нинішньому етапі розвитку криптовалют. Це передусім ідентифікація осіб, причетних до певних операцій із криптовалютами. Така ідентифікація має ефективно відбуватися у процесі попередження та розслідування злочинів. Інструменти для ідентифікації повинні бути доступними широкому колу правоохоронців, тому що ринок криптовалют постійно розширюється. Для кращого розуміння процесів у системі блокчейн інструменти для відповідного аналізу повинні містити належні засоби візуалізації та якомога повніші актуальні банки даних для правильної побудови асоціативних зв'язків із конкретними фізичними та юридичними особами. Крім наведеного, потрібно своєчасно проводити оцінку ризиків, пов'язаних із функціонуванням криптовалютних систем та їх обігом. У випадку виявлення відповідних загроз їх потрібно вчасно нейтралізувати з використанням інструментів технічного та юридичного характеру.

Список бібліографічних посилань

1. Kethineni S., Cao Y. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*. 2020. Vol. 30. Pp. 325–344. DOI: https://doi.org/10.1177/1057567719827051.

2. Nolasco Braaten C., Vaughn M. S. Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions. *Deviant Behavior*. 2019. URL: https://www.tandfonline.com/doi/full/10.1080/01639625.2019.1706706 (дата звернення: 13.12.2020).

3. Reddy E. Analysing the Investigation and Prosecution of Cryptocurrency Crime as Provided for by the South African Cybercrimes Bill. *Statute Law Review*. 2020. Vol. 41, Iss. 2. Pp. 226–239. DOI: https://doi.org/10.1093/slr/hmz001.

4. Teichmann F. M. J., Falker M.-C. Cryptocurrencies and financial crime: solutions from Liechtenstein. *Journal of Money Laundering Control*. 2020. URL: https://www.emerald.com/insight/content/doi/10.1108/JMLC-05-2020-0060 (дата звернення: 13.12.2020).

5. Kethineni S. Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms // The Palgrave Handbook of International Cybercrime and Cyberdeviance / eds. T. Holt, A. M. Bossler. Statesboro : Palgrave Macmillan, 2020. Pp. 305–326. DOI: https://doi.org/10.1007/978-3-319-78440-3.

6. Jiang J. K. Regulating Blockchain? A Retrospective Assessment of China's Blockchain Policies and Regulations. *Tsinghua China Law Review*. 2020. Vol. 12. Pp. 313–364. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654439 (дата звернення: 13.12.2020).

7. Albrecht C., Duffin K. M., Hawkins S., Morales Rocha V. M. The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*. 2019. Vol. 22, No. 2. Pp. 210–216. DOI: https://doi.org/10.1108/JMLC-12-2017-0074.

8. Kuzuno H., Karam C. Blockchain explorer: An analytical process and investigation environment for bitcoin // APWG Symposium on Electronic Crime Research (eCrime) (25–27 April 2017). 2017. Pp. 9–16. DOI: https://doi.org/10.1109/ECRIME.2017.7945049.

9. Balaskas A., Franqueira V. N. L. Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges // International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (11–12 June 2018). DOI: https://doi.org/10.1109/CyberSecPODS.2018.8560672.

10. Cremona K., Tabone D., De Raffaele C. Cremona. Cybersecurity and the Blockchain: Preventing the Insertion of Child Pornography Images // International Conference on Cyber-Enabled Distributed

Computing and Knowledge Discovery (CyberC) (17–19 October 2019). 2019. Pp. 197–204. DOI: https://doi.org/10.1109/cyberc.2019.00042.

Надійшла до редколегії 17.12.2020

НОСОВ В. В., МАНЖАЙ И. А. ОТДЕЛЬНЫЕ АСПЕКТЫ АНАЛИЗА КРИПТОВАЛЮТНЫХ ТРАНСАКЦИЙ ВО ВРЕМЯ ПРЕДУПРЕЖДЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Проведен анализ отдельных инструментов для визуализации движения криптовалютних ценностей, а также идентификации пользователей, совершивших соответствующие трансакции. Изучено преимущества и недостатки криптовалют с точки зрения правонарушителей и правоохранительных органов. Определены основные направления использования криптовалют в преступной среде. Проанализированы текущее состояние и перспективы нормативно-правового регулирования криптовалют в Украине. Изучены теоретические основы функционирования криптовалют. Раскрыты возможности отдельных сервисов, предназначенных для анализа криптовалютных трансакций. На примере работы сервиса «Crystal Expert» продемонстрирован процесс оценки рисков и построения визуальных цепочек криптовалютных трансакций. На основании проведенного анализа определены основные задачи для правоохранительных органов на современном этапе развития криптовалют.

Ключевые слова: *криптовалюта, анализ трансакций, визуализация, правоохранительные органы, противодействие преступности.*

NOSOV V. V., MANZHAI I. A. CERTAIN ASPECTS OF THE ANALYSIS OF CRYPTOCURRENCY TRANSACTIONS DURING THE PREVENTION AND INVESTIGATION OF CRIMES

The analysis of separate tools for the visualization of movement of cryptocurrency values, and also identification of users who carried out the corresponding transactions has been carried out. The advantages and disadvantages of cryptocurrency from the point of view of offenders and law enforcement agencies have been studied. The main directions of using cryptocurrency in a criminal environment have been determined. The current state and perspectives of normative and legal regulation of cryptocurrency in Ukraine have been analyzed. Theoretical principles of cryptocurrency functioning have been studied. The basic concepts used in this area have been revealed. The properties of cryptocurrency have been described. The mechanism of its issuance of guaranteeing pseudo-anonymity while working with cryptocurrency has been outlined. Some features of blockchain technology and formation of cryptocurrency addresses have been revealed. It has been noted that one of the first and most well-known cryptocurrency is bitcoin. The format of bitcoin address presentation has been described. It has been emphasized that bitcoin wallet software can operate with any number of addresses or each address can be served by a separate wallet. The technology of mixing transactions and the method of increasing the anonymity of CoinJoin have been described. The authors have revealed the possibilities of separate services intended for the analysis of cryptocurrency transactions (Maltego, Bitconeview, Bitiodine, OpReturnTool, Blockchain.info, Anyblockanalytics.com, Chainalysis, Elliptic, Ciphertrace, Blockchain Inspector). The process of risk assessment and construction of visual chains of cryptocurrency transactions has been demonstrated on the example of the “Crystal Expert” service. Different types of bitcoin addresses’ holders and risk levels have been described. The main and additional investigation tools used on the “Crystal Expert” platform have been revealed. Based on the conducted analysis, the authors have defined the main tasks for law enforcement agencies at the current stage of development of cryptocurrency. The basic requirements for tools designed for cryptocurrency analysis have been outlined. The authors have suggested some measures of law enforcement agencies’ respond to threats related to cryptocurrency.

Key words: *cryptocurrency, analysis of transactions, visualization, law enforcement agencies, crime prevention.*