

КРИМІНАЛЬНЕ ПРАВО ТА ПРОЦЕС, КРИМІНОЛОГІЯ, КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.13

DOI https://doi.org/10.32782/galician_studies/law-2024-5-6**Мовчан Анатолій Васильович,**

доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ
ORCID ID: 0000-0002-6997-6517

Козій Василь Васильович,

кандидат юридичних наук,
докторант кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ
ORCID ID: 0000-0002-8221-6678

УКЛАДЕННЯ УГОД У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ ПРО НЕЗАКОННЕ ЗАВОЛОДІННЯ КРИПТОВАЛЮТОЮ (ВІРТУАЛЬНИМИ АКТИВАМИ)

Статтю присвячено дослідженню укладення угод у кримінальному провадженні про незаконне заволодіння криптовалютою. Актуальність тематики обумовлена тим, що криптовалюти (віртуальні активи) упродовж останніх років набули значного поширення серед пересічних громадян. Відповідно у цій сфері суспільних відносин має місце і ріст злочинності, винні особи притягуються до кримінальної відповідальності, і серед інших, постає питання можливості та особливостей укладення угод у таких кримінальних провадженнях. У процесі дослідження застосовано формально-логічний метод, а також методи системного та техніко-юридичного аналізу. Наведено процесуальний інструментарій, яким наділений прокурор у контексті укладення угоди про визнання винуватості під час досудового розслідування злочинів, пов'язаних із незаконним заволодінням криптовалютою. Сформульовано правила про те, які обставини повинні враховуватися при укладенні угоди про визнання винуватості. Наведено особливості укладення угоди про примирення у кримінальному провадженні щодо незаконного заволодіння криптовалютою як під час досудового розслідування так і в суді. Запропоновано покроковий алгоритм фіксування повернення криптовалюти потерпілому або її перерахування на криптовалютні гаманці, які контролюються органами прокуратури або спеціально уповноваженими на зберігання криптовалюти органами. Сформульовано вимоги до того, які відомості та в якій послідовності мають бути відображені в угоді про визнання винуватості та в угоді про примирення, у разі їх укладання у кримінальному провадженні про незаконне заволодіння криптовалютою.

Ключові слова: криптовалюта, блокчейн, віртуальні активи, злочини у сфері криптовалют, незаконне заволодіння криптовалютою, розслідування незаконного заволодіння криптовалютою, угоди у кримінальному провадженні про незаконне заволодіння криптовалютою.

Movchan A. V., Kozii V. V. Conclusion of agreements in criminal proceedings regarding illegal possession of cryptocurrency (virtual assets)

The article is devoted to the study of the conclusion of agreements in criminal proceedings on the illegal possession of cryptocurrency. The topicality of the topic is due to the fact that cryptocurrencies (virtual assets) have gained significant popularity among ordinary citizens in recent years. Accordingly, in this sphere of social relations there is also an increase in crime, guilty persons are brought to criminal liability, and among others, the question of the possibility and features of concluding agreements in such criminal proceedings arises. In the research process, the formal-logical method, as well as methods of systemic and technical-legal analysis were applied. The procedural tools available to the prosecutor in the context of concluding a plea agreement during the pre-trial investigation of crimes related to the illegal acquisition of cryptocurrency are given. Rules have been formulated on what circumstances should be taken into account when entering into a plea agreement. The features of concluding a settlement agreement in criminal proceedings regarding the illegal possession of cryptocurrency both during a pre-trial investigation and in court are given. A step-by-step algorithm for fixing the return of cryptocurrency to the victim or its transfer to cryptocurrency wallets, which are controlled by

the prosecutor's office or bodies specially authorized to store cryptocurrency, is proposed. The requirements for what information and in what sequence should be reflected in the plea agreement and in the reconciliation agreement, in the case of their conclusion in criminal proceedings for illegal possession of cryptocurrency, have been formulated.

Key words: *cryptocurrency, blockchain, crimes in the field of cryptocurrencies, illegal possession of cryptocurrency, investigation of illegal possession of cryptocurrency, agreements in criminal proceedings on illegal possession of cryptocurrency.*

Актуальність проблеми. Упродовж останніх десятиліть відбувся гігантський розвиток сфери криптовалют у світі. Своїй без перебільшення тріумфальній ході технологія блокчейн, яка є основою будь-якої криптовалюти, завдячує таємничому творцю або групі творців під псевдонімом Сатоші Накамото, який у 2008 році створив першу криптовалюту – біткоїн. Історія біткоїна почалася з розміщення Сатоші Накамото статті «Bitcoin: A Peer-to-Peer Electronic Cash System», що в перекладі з англійської мови означає: «Біткоїн: електронна пірингова система готівки» у Cryptography Mailing List Email, де описано пірингову (peer-to-peer) версію системи цифрової готівки, яка забезпечує можливість надсилати онлайн-платежі напряму від однієї сторони до іншої, обминаючи будь-які фінансові установи [1].

Натомість задовго до створення біткоїна, у 1983 році Девід Чаум і Стефан Брендс пропонували перші протоколи функціонування електронної готівки [2].

Водночас ще до Сатоші Накамото ідею децентралізованої цифрової валюти у 1998 році описав Нік Сабо. Проте його розробка bit gold, яка багато в чому нагадує біткоїн, так і не знайшла свого втілення [3].

Ідею криптовалюти «b-money» описав у 1998 році Вей Дай в розісланні шифропанків. Зокрема, він зазначав про передбачення існування невідстежуваної (untraceable) мережі, де відправники та одержувачі визначені лише цифровим псевдонімом (тобто відкритими ключами), а повідомлення підписуються відправником та розшифровуються одержувачем [4].

Отже можна стверджувати, що біткоїн – це у тому числі реалізація також ідей Девіда Чаума і Стефана Брендса та пропозицій B-money від Вея Дая та Bit Gold від Ніка Сабо.

Станом на даний час існує декілька десятків тисяч криптовалют, а також і відповідно у сфері криптовалют вчиняється все більше і більше злочинів, пов'язаних із незаконним заволодінням криптовалютою.

У зв'язку з цим перед слідчими та прокурорами постає багато викликів, які стосуються передусім розслідування таких злочинів. Проте не менш важливим з практичної точки зору та наукової складовою є питання укладення угод у кримінальних провадженнях про незаконне заволодіння криптовалютою.

Аналіз останніх досліджень і публікацій. Окремі питання, які стосуються правового регулювання криптовалют (віртуальних активів), а також розслідування злочинів у сфері криптовалют містяться у працях Р. Й. Бачо, В. Д. Іванюк, І. С. Карпюка та О. В. Кузьменко, Д. В. Казначеевої та А. О. Дорош, О. В. Кремінського, А. Ю. Плюшкіна, В. О. Рядінської, Н. Хак Сіддікі та Р. О. Мовчана, В. В. Носова та І. А. Манжай, а також інших науковців.

Слід зазначити, що вітчизняні та закордонні дослідники, досліджуючи питання, пов'язані із розслідуванням злочинів у сфері криптовалют, приділяють увагу різним аспектам у цій сфері. Так, V. Duntu та O. Duкуj (2021), розглядаючи криптовалюту як інструмент фінансування тероризму відзначають, що для боротьби зі злочинністю головним питанням є деанонімізація власника/користувача Bitcoin, що дозволяє ідентифікувати злочинця [5].

Utkina M., Samsin R., Pochtovyі M. (2023), досліджуючи питання фінансової розвідки (моніторингу) операцій з віртуальними активами, констатують, що віртуальні активи використовуються в таких кримінальних правопорушеннях, як відмивання грошей, і визначають роль фінансової розвідки в ефективній боротьбі з відмиванням грошей [6].

Maurushat A. та Halpin D. (2022) розглядають криптовалюту як інструмент онлайн-шахрайства та аналізують виклики, пов'язані з розслідуванням шахрайства з криптовалютними інвестиціями [7].

Дослідження Phillips R., Wilder H. (2020), зокрема присвячено з'ясуванню питань про вчинення шахрайства з криптовалютою за допомогою фішингу [8].

Pengcheng Xia, Bowen Zhang, Ru Ji, Bingyu Gao, Lei Wu, Xiapu Luo, Haoyu Wang, Guoai Xu (2020) охарактеризували шахрайство під час обміну криптовалют [9].

Наукова праця Самойленко О. А. та Тітуніна К. В. (2023) присвячена типовим криміналістичним засобам розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют [10].

В. В. Носов та І. А. Манжай з'ясували окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. [11].

Натомість питання укладення угод у кримінальних провадженнях про незаконне заволодіння криптовалютою до цього часу залишається практично недослідженим науковцями.

Мета дослідження. Метою статті є з'ясування питань, пов'язаних з укладенням угод у кримінальному провадженні про незаконне заволодіння криптовалютою та пошук і знаходження способів вирішення наявних проблем.

Виклад основного матеріалу дослідження. Передусім потрібно в загальних рисах з'ясувати що таке криптовалюта, які її види та основи функціонування і обігу, а також яким процесуальним інструментарієм КПК України наділяє прокурора щодо укладення угод у кримінальному провадженні про незаконне заволодіння криптовалютою та що саме потрібно враховувати при цьому.

Автором терміну криптовалюта є оглядач видання «Форбс» Енді Грінберг, який у 2011 році описав технологічні переваги електронної готівки [12].

Криптовалюта є різновидом цифрової валюти, емісія та облік якої відбувається у децентралізованій платіжній системі в автоматичному режимі, який гарантує відсутність єдиного адміністратора. Практично будь-яка особа може бути власником тієї чи іншої криптовалюти, маючи банківську картку та доступ до мережі Інтернет. Процес покупки криптовалюти на онлайн біржі чи обмінному ресурсі та переведення її на власний електронний гаманець займає від кількох секунд і є зручною операцією. Досить поширеною є торгівля криптовалютами на різних централізованих (СЕХ) та децентралізованих (DeFi, DEX) онлайн-біржах. Придбавши певну кількість криптовалюти, її можна використати для стейкінгу – отримання певної кількості криптовалюти за її блокування у блокчейні, синхронізувавши електронний гаманець за допомогою програмного забезпечення із відповідними сервісами, що є аналогом класичного банківського депозиту. У середовищі індустрії криптовалют всі інші, створені після біткоїна криптовалюти, називають алькоїнами. Деякі з них є його форками, тобто видозміненим біткоїном, оскільки за основу їх функціонування взято програмний код біткоїна, але із певними відмінностями. На відміну від Біткоїна інша найбільш відома криптовалюта Ефіріум є програмованим блокчейном, який дає змогу створювати і розгортати децентралізовані додатки (DApps), а також смарт-контракти. Криптовалюти також поділяються на децентралізовані та стейблкоїни. Курс децентралізованих постійно змінюється, у той час як курс стейблкоїнів є відносно стабільним і загалом відповідає вартості активу, який його забезпечує, наприклад 1 USD. Також в індустрії криптовалют функціонують токени, які можна віднести до грошового сурогату або одиниці обліку на цифровому балансі, яка випускається як централізовано, так і децентралізовано та не завжди базується на технології блокчейну. Як правило, токени посвідчують право на щось.

Іншим видом криптовалюти є NFT, тобто невзаємозамінні токени, які від інших віртуальних активів відрізняються тим, що вони є неповторними, єдиними у своєму роді. NFT або Non-Fungible Token, у перекладі з англійської означає невзаємозамінний токен – це унікальний токен, який існує в єдиному екземплярі і його не можна нічим замінити та який засвідчує право власника на цифровий актив. Наприклад, якщо 1 Ефіріум дорівнює іншому 1 Ефіріусу, то таке правило до невзаємозамінних токенів не діє. NFT реєструється у мережі, де відображається його назва і те, чим він є (графічне зображення, мелодія, гра, доменні імена, бренди чи щось інше). Цілком слушно зазначає Аніта К. Шарма про те, що NFT – це лише посвідчувальний сертифікат у цифровій формі, який підтверджує право власності на інший відповідний цифровий (віртуальний) актив [13].

Як ми вказували раніше, будь-яка криптовалюта умовно складається із набору символів – букв та цифр, і при цьому із цих самих символів складається адреса гаманця, так званий публічний ключ, який генерується системою і який потрібно знати тому, хто збирається переказати на нього певну суму тієї чи іншої криптовалюти. Наприклад, адреса електронного гаманця біткоїну може мати наступний вигляд: 1JNzanNTkCLF4VrMct3ByuLu5nje3Zvq1i. Проте є ще приватний ключ, який не можна передавати нікому, так як останній дозволяє у блокчейні біткоїну підтвердити, що відповідна кількість криптовалюти знаходиться на вказаному гаманці, тобто за вказаною адресою в блокчейні. Володіти криптовалютою можна, якщо мати електронний гаманець та приватні ключі. У випадку ж коли криптовалюта знаходиться на біржі, то і приватні ключі теж знаходяться у біржі, і у випадку зламу біржі чи викрадення з неї криптовалюти відповідно власник її також втрачає [14, с. 181].

Натомість Д. В. Казначеева та А. О. Дорош вказують, що криптовалюта функціонує завдяки механізму асиметричного шифрування. Одиниця криптовалюти – це код, який народжується в результаті

складних комп'ютерних математичних обчислень. Операція з утворення (видобутку) криптовалюти називається майнінгом. Термін «майнінг» прийшов з англійської мови та дослівно означає «видобуток корисних копалин». На практиці майнінг – це формування нових блоків у блокчейн-ланцюги кожної криптовалюти. Крім цього, майнінг також можна охарактеризувати як процес запису всіх здійснених транзакцій криптовалюти в їх блокчейн, відкриту базу даних здійснених операцій. Якщо розглянути роботу будь-якої криптовалюти, то майнінг можна назвати основною функцією для фундаментальної будови всієї внутрішньої структури крипто. Завдяки майнінгу формуються нові блоки із записами про вчинені транзакції і підтримується емісія криптовалюти (за рахунок винагороди майнерам). Процес майнінгу – це знаходження числа «nonce», яке дозволяє майнеру сформувати блок із записами про проведені транзакції і ввести його в блокчейн-ланцюжок. За створення кожного чергового блоку в блокчейні (структурної одиниці із записами про перекази) для майнера передбачено винагороду за рахунок емітованих монет. Майнінг – це єдиний спосіб підтримки роботи мережі криптовалюти, а також для її емісії і поширення. Таким чином, на нашу думку, криптовалюта – це цифрова валюта, яка ґрунтується на застосуванні криптографії для створення і контролю нових одиниць валюти і здійснення транзакцій. Оскільки криптовалюта не підлягає централізованому регулюванню, її можна віднести до віртуальної валюти, тобто засобу вираження вартості, яким можна торгувати в цифровій формі [15, с. 172–173].

Погоджуючись із наведеним вище, слід зауважити, що крім майнінгу, тобто технології прув оф ворк (POW) завдяки якому можна за допомогою спеціалізованого обладнання згенерувати певну кількість одиниць тієї чи іншої криптовалюти, багато криптовалют базуються на технології прув оф стейк (POS) – коли завдяки наявності у володінні певної кількості криптовалюти, яка блокується за допомогою спеціалізованого програмного забезпечення можна отримувати певну кількість цієї самої криптовалюти як прибуток по аналогії з банківським депозитом.

Відповідно до ухваленого 17.02.2022 Закону України «Про віртуальні активи», під віртуальним активом законодавець фактично визнає криптовалюту, і згідно з п. 1 ст. 1 останнього віртуальний актив визначено як нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі [16].

Як засвідчило опитування 220 прокурорів – процесуальних керівників у кримінальних провадженнях з приводу того, як вони ставляться до можливості укладення угод у кримінальному провадженні про незаконне заволодіння криптовалютою, 98% опитаних відзначили, що у цій категорії укладення угод є доцільним. Проте жодний із опитаних такі угоди не укладав.

КПК України не передбачає жодних особливостей щодо укладення угод у кримінальних провадженнях про незаконне заволодіння криптовалютою, отже будь-які питання, які виникають при укладенні угод і які не регламентовані кримінальним процесуальним законом повинні вирішуватися з урахуванням загальних засад кримінального провадження, як це вказано у ч. 6 ст. 9 КПК України. Отже, укладення угод у кримінальних провадженнях цієї категорії повинно відповідати положенням Глави 35 КПК України. Аналіз норм КПК України, які містяться у Главі 35 дозволяє сформулювати такі правила та підходи до укладення угод у кримінальних провадженнях про незаконне заволодіння криптовалютою. Обставини, які враховуються прокурором при укладенні угоди про визнання винуватості, сформульовані у ст. 470 КПК України і відповідно ними є: 1) ступінь та характер сприяння підозрюваного чи обвинуваченого у проведенні кримінального провадження щодо нього або інших осіб; 2) характер і тяжкість обвинувачення (підозри); 3) наявність суспільного інтересу в забезпеченні швидшого досудового розслідування і судового провадження, викритті більшої кількості кримінальних правопорушень; 4) наявність суспільного інтересу в запобіганні, виявленні чи припиненні більшої кількості кримінальних правопорушень або інших більш тяжких кримінальних правопорушень.

Стосовно ступеню та характеру сприяння підозрюваного чи обвинуваченого у проведенні кримінального провадження щодо нього або інших осіб, то ключовою обставиною, яка має при цьому враховуватися – це згода підозрюваного (обвинуваченого) на повернення криптовалюти, якою він незаконно заволодів, а також викриття співучасників вчинення кримінального правопорушення та допомога у поверненні, і зрештою повернення криптовалюти, яка знаходиться під їх контролем, тобто до якої вони мають доступ і можуть нею розпоряджатися. Також в окремих випадках це може бути розкриття способу вчинення злочину, його технічної кіберскладової. Якщо цих вимог не дотримано, то про угоду про визнання винуватості не повинно йтися взагалі. Із цим погодилися 88% із 220 опитаних прокурорів – процесуальних керівників. Водночас при вирішенні питання укладення цього виду угод у вказаній категорії кримінальних проваджень слід застосовувати гнучкий підхід, і якщо наявний суспільний

інтерес у забезпеченні швидшого досудового розслідування і судового провадження та викритті більшої кількості кримінальних правопорушень, які у тому числі вчинені іншими особами, то очевидно що така угода може бути укладена. Це саме стосується і врахування наявності суспільного інтересу в запобіганні, виявленні чи припиненні більшої кількості кримінальних правопорушень або інших більш тяжких кримінальних правопорушень.

Стосовно угоди про примирення у кримінальних провадженнях цієї категорії, то визначальним для затвердження такої угоди судом, і відповідно для укладення має бути дотримання вимог ст. 471 КПК України, а саме передбачення в угоді відшкодування завданої шкоди чи переліку дій, не пов'язаних з відшкодуванням шкоди, які підозрюваний чи обвинувачений зобов'язані вчинити на користь потерпілого та строк їх вчинення. Тобто в угоді має бути вказано, яку кількість та якої саме криптовалюти підозрюваним чи обвинуваченим має бути повернуто та на які саме адреси електронних гаманців та в який строк.

Проте про угоду не повинно йтися у тому випадку, коли слідчий чи прокурор мають достатню доказову базу щодо конкретного підозрюваного чи обвинуваченого, а також щодо інших осіб, або коли під час затримання особи та в подальшому під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, наприклад обшуків, затримань, оглядів оперативні працівники, слідчий чи прокурор отримали доступ до викраденої криптовалюти, тобто до сід фраз, паролів від криптовалютних гаманців і т. ін., а також у випадках коли їм достовірно відомо про те, яким саме способом вчинено кримінальне правопорушення (йдеться про технічні кібераспекти з метою усунення технічних недоліків, щоб у подальшому інші особи не змогли ними скористатися).

Розглянемо можливість і доцільність укладення угоди про визнання винуватості на прикладі справи, про яку наявне повідомлення від 07.03.2023 на порталі МВС. Відповідно до останнього, зловмисники розповсюджували шкідливе програмне забезпечення, яке зашифровувало дані на техніці потерпілих. За відновлення доступу вимагали викуп у криптовалюті. Кіберполіція викрила учасника хакерської групи, причетної до завдання європейським компаніям 40 млн євро збитків. 39-річний громадянин України, який наразі мешкає у Німеччині, причетний до масштабних кібератак з використанням програми-вимагача Doppel Raumer. Атаки цим вірусом стали можливими завдяки поширеному шкідливому програмному забезпеченню EMOTET. Програму-вимагач розповсюджували різними каналами, зокрема через фішингові та спам-розсилки з прикріпленими документами, що містили шкідливий код – JavaScript або VBScript. Потрапивши на техніку, шкідлива програма криптувала дані, а за відновлення доступу зловмисники вимагали викуп [17].

Очевидно, що про угоду у вказаному провадженні може йтися лише у випадку згоди підозрюваного співпрацювати з слідчим чи прокурором та повідомлення ним даних про інших учасників угруповання, їх місцезнаходження, інші вчинені злочини та способи їх вчинення, а також у випадку його згоди повернути одержану від потерпілих криптовалюту.

В іншому випадку, за повідомленням GSMinfo від 27.03.2024, українець зміг незаконно намайнити криптовалюти на 2 мільйони доларів. Європол затримав 29-річного українця, ім'я якого не розголошується, за підозрою в організації масштабної операції з викрадення криптовалют. Його звинувачують у масовому використанні ресурсів хмарних обчислень, що належать іншим особам, шляхом розгортання мільйона віртуальних серверів через зламані акаунти для несанкціонованого майнінгу криптовалют. Розслідування показало, що підозрюваний діяв з 2021 року, використовуючи самостійно розроблені брутфорс-інструменти для викрадення 1 500 акаунтів дочірньої компанії провідного світового постачальника послуг електронної комерції. За допомогою цих зламанних акаунтів хакеру вдалося отримати адміністративний доступ, створити понад мільйон віртуальних машин для незаконного видобутку криптовалют, використовуючи ресурси, які йому не належали [18].

У цьому провадженні про угоду також може йтися лише у випадку згоди підозрюваного співпрацювати із слідчим чи прокурором та його згоди повернути одержану від незаконної діяльності криптовалюту.

Також важливе значення має і подальше розпорядження віртуальними активами після того, як підозрюваний або обвинувачений або надасть до них доступ слідчому, прокурору або іншій спеціально визначеній або уповноваженій особі, адже ринок криптовалют надзвичайно волатильний і сповнений несподіванок, адже з часом одні криптовалюти йдуть у небуття, адже виявляються або скамом або повністю провальними проектами, а інші процвітають і сягають неймовірних висот в ціні та з точки зору технічних і економічних рішень. Так, згідно з повідомленням Forbes, на сьогодні існує щонайменше

50 блокчейнів, чия ринкова вартість перевищує \$1 млрд. Близько двох десятків із них автори називають «функціональними зомбі». Ці проекти використовують амбітні описи для своєї діяльності: від універсального суперкомп'ютера до невідстежуваної платіжної мережі, йдеться в матеріалі. Однак за сукупної вартості понад \$116 млрд, активність у цих блокчейнах залишається мінімальною, вважають у медіа. Серед мереж, які потрапили до переліку «живих мерців», значаться проекти: Ethereum Classic; Bitcoin SV; Litecoin; Algorand; Monero; Bitcoin Cash; Fantom; Cardano; Tezos; Stellar та інші. При цьому аналітики підкреслюють, що вони вказали лише на основні блокчейни. Загальна кількість «зомбі-проектів» обчислюється сотнями, а кількість неспроможних активів – тисячами [19].

Звідси слідує одне просте правило: після укладення угоди та одержання доступу до віртуальних активів ризики її зберігання та розпорядження повністю переходять на слідчого, прокурора або посадову особу спеціально уповноваженого органу. У цьому випадку можливі три типові ситуації щодо подальшої зміни їх вартості: 1) вартість буде залишатися приблизно такою самою як і в момент перерахування; 2) вартість значно знизиться, можливо навіть до нуля; 3) вартість може збільшитися в десятки чи навіть сотні разів і вирахувати наперед, який із цих сценаріїв відбудеться, практично неможливо. Тому єдиним правильним рішенням є обмін такої критпocurrency на фіатну валюту із її подальшим зарахуванням на спеціальні банківські рахунки органу досудового розслідування, прокуратури чи спеціально створеного державного органу. Більше того, в умовах угоди з підозрюваним чи обвинуваченим можна передбачити чіткий та поетапний алгоритм дій, який буде винений останніми, і відповідно до якого вони наприклад, самостійно спочатку перераховують незаконно одержану криптовалюту із електронних гаманців, які ними контролюються на визначені в угоді біржу чи інший онлайн сервіс, де проводять її обмін на фіатну валюту і в подальшому із біржі чи іншого сервісу перераховують фіатну валюту (долари США, євро чи ін.) на вказаний слідчим чи прокурором банківський рахунок, який належить державі (у випадку угоди з про примирення – потерпілому).

Висновки і перспективи подальших досліджень. Отже, укладення угод у кримінальному провадженні про незаконне заволодіння криптовалютою є важливим процесуальним інструментом, завдяки якому незаконно здобута (викрадена) криптовалюта може бути повернута потерпілому або вилучена та в подальшому конфіскована в дохід держави.

Важливе значення при укладенні угод у цій категорії кримінальних проваджень має згода підозрюваного (обвинуваченого) на повернення криптовалюти, якою він незаконно заволодів, а також викриття співучасників вчинення кримінального правопорушення та допомога у поверненні, і зрештою повернення криптовалюти, яка знаходиться під їх контролем.

В угоді має бути вказано, яку кількість та якої саме криптовалюти підозрюваним чи обвинуваченим має бути повернуто та на які саме адреси електронних гаманців та в який строк. Але слід враховувати і те, що після укладення угоди та одержання доступу до віртуальних активів ризики її зберігання та розпорядження повністю переходять на слідчого, прокурора або посадову особу спеціально уповноваженого органу. І вартість криптовалюти може суттєво коливатися як у бік зменшення, так і в бік збільшення. Тому правильним вирішенням такої ситуації є обмін такої криптовалюти на фіатну валюту із її подальшим зарахуванням на спеціальні банківські рахунки органу досудового розслідування, прокуратури чи спеціально створеного державного органу. В умовах угоди з підозрюваним чи обвинуваченим можна передбачити чіткий та поетапний алгоритм дій, відповідно до якого вони, наприклад, самостійно спочатку перераховують незаконно одержану криптовалюту із електронних гаманців, які ними контролюються, на визначені в угоді біржу чи інший онлайн сервіс, де проводять її обмін на фіатну валюту і в подальшому із біржі чи іншого сервісу перераховують вже фіатну валюту.

В угоді має бути зазначено назву криптовалюти, її кількість у кожній з транзакцій, якщо їх декілька, алгоритм хешування, якщо йдеться про альткоїни. Крім того, має бути визначено хто і яким чином сплачує плату за транзакцію, та в якому розмірі. Запропоновано укладення угоди та зазначення в її умовах альтернативного механізму обміну підозрюваним або обвинуваченим визначеної кількості криптовалюти на фіатну валюту та переказ на банківський рахунок, який контролюється державою, визначеного еквіваленту у фіатній валюті.

При укладенні угод у цій категорії кримінальних проваджень необхідно враховувати два ключові чинники: 1) умови та порядок повернення викраденої криптовалюти або її грошового еквіваленту; 2) умови та порядок, а також характер та особливості подальшої співпраці підозрюваного (обвинуваченого) із органом досудового розслідування, прокурором або іншим правоохоронним або державним органом, якщо йдеться про повідомлення технічних та інших даних, які стосуються можливості

незаконного заволодіння криптовалютою, допомоги у викритті інших осіб, які вчиняють злочини у сфері криптовалют; надання консультацій та допомоги у сфері криптовалют загалом.

Література

1. Накамото Сатоші Біткоїн: електронна пірингова система готівки. 2008. URL: https://bitcoin.org/files/bitcoin-paper/bitcoin_uk.pdf.
2. Chaum David. Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto*. 1983. 82 (3). P. 199–203.
3. Szabo Nick. Bit Gold. Unenumerated. *Blogspot*. 2005. URL: <http://unenumerated.blogspot.com/2005/12/bit-gold.html>.
4. Вей Дай. Опис протоколу криптовалюти «b-money». URL: http://tango.ucoz.de/load/perevod_pervogo_opisanija_protokola_kripto_valjuty/1-1-0-1.
5. V. Dyntu., O. Dykyj Cryptocurrency as an instrument of terrorist financing. *Baltic journal of economic studies*. 2022, Vol. 7, No. 5. doi 10.30525/2256-0742/2021-7-5-67-72.
6. Utkina M., Samsin R., Pochtovyi M. Financial intelligence (monitoring) of the transactions with virtual assets: new legislation and best practices of foreign countries. *Journal of Money Laundering Control*, 2023. Vol. 26 No. 2, pp. 349–360. <https://doi.org/10.1108/JMLC-12-2021-0136>.
7. A. Maurushat, D. Halpin. Investigation of Cryptocurrency Enabled and Dependent Crimes. *Law, Governance and Technology Series*, 2022. Vol. 47, p. 235–267.
8. Phillips R., Wilder H. Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. doi 10.1109/ICBC48266.2020.9169433.
9. Wang H., Zhang, B., Ji, Ru Gao, Bingyu, Wu, Lei, Luo, Xiapu Xu, Guoai haracterizing cryptocurrency exchange scams. *Computers and Security*. 2020, Vol. 98, No. 101993 doi 10.1016/j.cose.2020.101993.
10. Самоїленко О. А., Тітуніна К. В. Типові криміналістичні засоби розслідування кримінальних правопорушень, пов'язаних із використанням криптовалют. *Актуальні питання у сучасній науці*. 2023. № 7 (13). С. 409–420. [https://doi.org/10.52058/2786-6300-2023-7\(13\)-409-420](https://doi.org/10.52058/2786-6300-2023-7(13)-409-420).
11. В. В. Носов, І. А. Манжай. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1 (80). С. 93–100.
12. Andy Greenberg. Crypto Currency. URL: <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-cryptocurrency.html#718ca248353e>.
13. Scott Reeves. NFTs Can Be Trojan Horse for Buyers. *Newsweek*. 2021. URL: <https://www.newsweek.com/nftscan-trojan-horse-buyers-pc-sales-pandemic-surge-continues-1595967>.
14. Мовчан А. В., Козій В. В. Основи розслідування злочинів щодо незаконного заволодіння криптовалютою. *Наука і правоохорона*. 2022. № 4 (58). С. 178–189. URL: [https://doi.org/10.36486/np.2022.4\(58\)](https://doi.org/10.36486/np.2022.4(58)).
15. Казначеева Д. В., Дорош А. О. Криптовалюта: проблеми правового регулювання. *Вісник кримінологічної асоціації України*. 2020. № 2 (23). С. 170–176.
16. Про віртуальні активи: Закон України від 17 лютого 2022 р. № 2074-IX. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>.
17. Кіберполіція викрила учасника хакерської групи, причетної до завдання європейським компаніям 40 млн євро збитків. URL: <https://mvs.gov.ua/uk/news/kiberpoliciia-vikrila-ucasnika-hakerskoyi-grupi-pricetnoyi-dozavdannia-jevropeskim-kompaniiam-40-mln-jevro-zbitkiv>.
18. Українець зміг незаконно намаїнити криптовалюту на 2 мільйони доларів. URL: <https://gsminfo.com.ua/162754-ukrainecz-zmig-nezakonno-namajnytu-kryptovalyuty-na-2-miljony-dolariv.html>.
19. Криптозомбі на сотні мільярдів доларів. Як зростання біткоїна відроджує ринок блокчейну? URL: <https://forbes.ua/innovations/kriptozombi-na-milyardi-dolariv-yak-blokcheyni-iz-nadnizkim-rivnem-koristuvannya-i-dali-protsvitayut-28032024-20201>.

References

1. Nakamoto Satoshi (2008). Bitcoin: elektronna pirynhova systema hotivky [Bitcoin: an electronic peering cash system]. Retrieved from: https://bitcoin.org/files/bitcoin-paper/bitcoin_uk.pdf [in Ukrainian].
2. Chaum, David (1983). Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto*. 82 (3). P. 199–203. [in English].
3. Szabo, Nick. Bit Gold (2005). Unenumerated. *Blogspot*. Retrieved from: <http://unenumerated.blogspot.com/2005/12/bit-gold.html> [in English].
4. Vei Dai. Opys protokolu kryptovalyuty «b-money» [Description of the «b-money» cryptocurrency protocol]. Retrieved from: http://tango.ucoz.de/load/perevod_pervogo_opisanija_protokola_kripto_valjuty/1-1-0-1 [in Ukrainian].
5. V. Dyntu., & O. Dykyj (2022). Cryptocurrency as an instrument of terrorist financing. *Baltic journal of economic studies*. 2022, Vol. 7, No. 5. doi 10.30525/2256-0742/2021-7-5-67-72 [in English].

6. Utkina, M., Samsin, R., & Pochtovyi, M. (2023). Financial intelligence (monitoring) of the transactions with virtual assets: new legislation and best practices of foreign countries. *Journal of Money Laundering Control*, Vol. 26 No. 2, pp. 349–360. <https://doi.org/10.1108/JMLC-12-2021-0136> [in English].
7. A. Maurushat, & D. Halpin (2022). Investigation of Cryptocurrency Enabled and Dependent Crimes. *Law, Governance and Technology Series*, Vol. 47, p. 235–267 [in English].
8. Phillips, R., & Wilder, H. (2020). Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. doi 10.1109/ICBC48266.2020.9169433 [in English].
9. Wang, H., Zhang, B., Ji, Ru Gao, Bingyu, Wu, Lei, Luo, & Xiapu Xu, (2020). Guoai haracterizing cryptocurrency exchange scams. *Computers and Security*. 2020, Vol. 98, No. 101993 doi 10.1016/j.cose.2020.101993 [in English].
10. Samoilenko, O.A., & Titunina, K.V. (2023). Typovi kryminalistychni zasoby rozsliduvannia kryminalnykh pravoporushen, poviazanykh iz vykorystanniam kryptovaliut [Typical forensic means of investigating criminal offenses related to the use of cryptocurrencies]. *Aktualni pytannia u suchasni nautsi – Current issues in modern science*. No. 7 (13). 2023. P. 409–420. Retrieved from: [https://doi.org/10.52058/2786-6300-2023-7\(13\)-409-420](https://doi.org/10.52058/2786-6300-2023-7(13)-409-420) [in Ukrainian].
11. V.V. Nosov, & I.A. Manzhai (2021). Okremi aspekty analizu kryptovaliutnykh transaktsii pid chas poperedzhennia ta rozsliduvannia zlochyniv [Certain aspects of the analysis of cryptocurrency transactions during the prevention and investigation of crimes]. *Pravo i bezpeka – Law and security*. No. 1 (80), P. 93–100 [in Ukrainian].
12. Andy Greenberg (2011). Crypto Currency. Retrieved from: <https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-cryptocurrency.html#718ca248353e> [in English].
13. Scott Reeves. NFTs Can Be Trojan Horse for Buyers. *Newsweek* (2021). Retrieved from: <https://www.newsweek.com/nftscan-trojan-horse-buyers-pc-sales-pandemic-surge-continues-1595967> [in English].
14. Movchan, A.V., & Kozii, V.V. (2022). Osnovy rozsliduvannia zlochyniv shchodo nezakonnoho zavolodinnia kryptovaliutoiu [The basics of investigating crimes related to the illegal acquisition of cryptocurrency]. *Nauka i pravookhorona - Science and law enforcement*. No. 4 (58). P. 178–189. Retrieved from: [https://doi.org/10.36486/np.2022.4\(58\)](https://doi.org/10.36486/np.2022.4(58)) [in Ukrainian].
15. Kaznacheieva, D.V., & Dorosh, A.O. (2020). Kryptovaliuta: problemy pravovoho rehulivannia [Cryptocurrency: problems of legal regulation]. *Visnyk kryminolohichnoi asotsiatsii Ukrainy – Bulletin of the Criminological Association of Ukraine*. No. 2 (23). P. 170–176 [in Ukrainian].
16. Verkhovna Rada of Ukraine (2022). Pro virtualni aktyvy: Zakon Ukrainy Zakon Ukrainy vid 17 liutoho 2022 r. № 2074-IX [About virtual assets: Law of Ukraine Law of Ukraine dated February 17, 2022 No. 2074-IX]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> [in Ukrainian].
17. Kiberpolitsiia vykryla uchasnyka khakerskoi hrupy, prychetnoi do zavdannia yevropeiskym kompaniiam 40 mln yevro zbytkiv [The cyber police exposed a member of a hacker group involved in the assignment of 40 million euros in damages to European companies]. Retrieved from: <https://mvs.gov.ua/uk/news/kiberpoliciia-vikryla-ucasnika-kakerskoyi-grupi-pricetnoyi-do-zavdannia-jevropeiskim-kompaniiam-40-mln-jevro-zbitkiv> [in Ukrainian].
18. Ukrainets zmih nezakonno namainyty kryptovaliuty na 2 miliony dolariv [A Ukrainian was able to illegally mine 2 million dollars worth of cryptocurrencies]. Retrieved from: <https://gsminfo.com.ua/162754-ukrayinecz-zmig-nezakonno-namainyty-kryptovalyuty-na-2-miljony-dolariv.html> [in Ukrainian].
19. Kriptozombi na sotni miliardiv dolariv. Yak zrostannia bitkoina vidrodzhuie rynek blokcheinu? [Cryptozombies worth hundreds of billions of dollars. How is Bitcoin's rise reviving the blockchain market?] Retrieved from: <https://forbes.ua/innovations/kriptozombi-na-milyardi-dolariv-yak-blokcheyni-iz-nadnizkim-rivnem-koristuvannya-i-dali-protsvitayut-28032024-20201> [in Ukrainian].