УДК 343.9

Ольга Карапетян,
кандидат економічних наук, доцент кафедри економічної безпеки та фінансових розслідувань юридичного факультету Тернопільського національного економічного університету

Віталій Білинський,
магістр кафедри економічної безпеки та фінансових розслідувань юридичного факультету Тернопільського національного економічного університету

ЗЛОЧИННІ ТЕХНОЛОГІЇ ЗБАГАЧЕННЯ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТ ТА ОСОБЛИВОСТІ ЇХ РОЗСЛІДУВАННЯ

Визначено переваги та недоліки використання та обігу криптовалюти, на основі чого обґрунтовано положення про зменшення корупційних ризиків за допомогою децентралізації цифрової валюти. Визначено практичні підходи до фінансових розслідувань незаконно одержаних коштів та обґрунтовано їх основні складові.

Ключові слова: *криптовалюта, злочинні технології, економічна злочинність, економічна безпека, фінансові розслідування, розшук активів.*

Карапетян О.

Преступные технологии обогащения с использованием криптовалют и особенности их расследования

Определены преимущества и недостатки использования и обращения криптовалюты, на основе чего обосновано положение об уменьшении коррупционных рисков с помощью децентрализации цифровой валюты. Определены практические подходы к финансовым расследованием незаконно полученных средств и обосновано их основные составляющие.

Ключевые слова: *криптовалюта, преступные технологии, экономическая преступность, экономическая безопасность, финансовые расследования, розыск активов.*

Karapetian O.

Criminal warranties with circular use and peculiarities of their investigation

The article outlines the advantages and disadvantages of the use and circulation of cryptographic commodities on the basis of which the provision on reduction of corruption risks by means of decentralization of the digital currency is substantiated. Practical approaches to financial investigations of illegally received funds are determined and their main components are substantiated.

Keywords: *cybercriminals, criminal technologies, economic crime, economic security, financial investigations, asset searches.*

Постановка проблеми. Впродовж останніх років систему фінансових платежів охопила хвиля технологічних інновацій, пов'язана з розвитком новітніх методів цифрових платежів. Застосування віртуальних інструментів збільшують ризики, пов'язані з можливостями відмивання грошей та фінансування тероризму, оскільки побудовані на передових технологіях схеми можуть бути використані в злочинних цілях. Сучасні технології розвиваються в геометричній прогресії, у той час як законодавче забезпечення потребує оперативності та миттєвої адаптованості. Часові лаги та різниця в темпах розвитку породжує відповідні прогалини, які використовують злочинці для особистого збагачення.

Фінансові трансакції, в яких раніше обов'язково були присутні гроші або деривативи, зараз можуть здійснюватися на основі нових технологій. Вони позначалися на ефективності методів розслідування фінансових злочинів, опиралися на емпіричні дослідження (коли для проведення трансакції була потрібна готівка або чеки та банківські рахунки), а також покладалися на те, що фінансові установи будуть дотримуватися своїх обов'язків (know your customer, KYC). Розроблені упродовж останніх років нові методи платежів можуть зруйнувати дієвість попередніх методів та поставити нові виклики перед організацією фінансових розслідувань з точки зору способів їх проведення.

Аналіз останніх досліджень і публікацій. Дослідженням розвитку та функціонування криптовалюти в системі знань присвячені праці таких дослідників, як: А. Гервайс, Д. Грубер, О. Караме, Н. Коуртоіс, Г. Максвел. Особливості застосування цифрової валюти відображені у працях О. Галицького, А. Квітки, І. Лубенця, О. Мороза.

Формулювання цілей статті. На основі аналізу міжнародного досвіду механізму боротьби з економічною злочинністю зарубіжних країн дослідити особливості національної та міжнародної практики розвитку феномену криптовалюти та особливостей здійснення фінансових розслідувань економічних злочинів, пов'язаних із використанням криптовалюти.

Виклад основного матеріалу дослідження. Трансформація видів грошей зумовлена впливом закономірного розвитку суспільства. Новий вид грошей визначається економічною необхідністю, коли попередні види грошей починають гальмувати процес виробництва і обміну, при умовах якщо сформувалися передумови для їх появи в процесі постійного пошуку більш економічних грошових систем, при яких відбувається економія суспільної праці, зниження витрат грошового обороту, підвищення швидкості обороту, збільшення надійності та зручності руху грошей.

Заборони на розрахунки готівкою понад установлений ліміт застосовуються з метою оптимізації платіжного обороту, дозволяючи скоротити використання готівки при здійсненні великих покупок. Досить жорсткі обмеження готівкового грошового обороту існують в США – 5 тис. дол., в Італії – 1 тис. євро, у Франції з 1 вересня 2015 р. діє обмеження в 1 тис. євро [1]. Введені обмеження були здійснені в рамках боротьби з фінансуванням тероризму (табл.1).

Таблиця 1

Обмеження щодо здійснення готівкових платежів у країнах світу, визначені у законодавстві [1]

Країна	Сума обмежень на платежі готівкою
Іспанія	3 000 євро
Греція	500 євро
ПАР	425 дол. США
Індія	450 дол. США
Південна Корея	4 000 дол. США
Китай	7 400 дол. США
Великобританія	9 000 фунтів стерлінгів

В цьому контексті в глобальній фінансовій системі активно обговорюється проблема використання цифрових грошей або криптовалюти.

Біткоїн став першим практичним доказом успішної роботи Blockchain-системи. Однак сама технологія Blockchain набагато ширша, ніж криптовалюта, вона дозволяє створювати практично будь-які розподілені системи обліку. Наприклад, це можуть бути земельні реєстри, нотаріальні послуги, посвідчення особи, системи обліку акцій та інших прав власності.

Система запровадження нових можливостей призводить до нових ризиків. Криптовалюта ставить перед державними структурами нові виклики у боротьбі зі злочинністю, тероризмом та легалізацією доходів, отриманих злочинним шляхом. При цьому успішного прикладу запровадження регулювання криптовалюти у світі досі немає. Переваги та недоліки її використання відображені у табл. 2.

Великим викликом для служби фінансового моніторингу є так звані анонімні криптовалюти. Серед найбільш функціональніших та розповсюджених криптовалют можна виділити Monero, Dash та особливе місце серед анонімних валют займає Zcash.

Таблиця 2

Оцінка сутності, переваги та недоліки використання Bitkoin*

Сутнісна визначеність в різних джерелах інформації	Переваги	Недоліки
• Криптовалюта – миттєва і надійна система платежів і грошових переказів, заснована на новітніх технологіях і непідконтрольна урядовим інституціям (Bitcoin Security); • криптовалюта – вид цифрових грошей, в якому використовуються розподілені мережі та публічно доступні журнали реєстрації угод, а основні ідеї криптографії поєднані в них з грошовою системою (Insider.pro); • криптовалюта – вид цифрової валюти, заснований на складних обчисленнях деякої функції, яку легко перевірити зворотними математичними діями, в основі емісії якої є принцип доказу виконання роботи «Proof-of-work»; • криптовалюта – засіб обміну, як і звичайні валюти, але призначена для обміну цифровою інформацією, що стало можливим завдяки певним принципам криптографії (CryptoCoins News).	• Абсолютна анонімність; • відсутність оподаткування і комісій; • миттєві переводи; • неможливість підробки; • міжнародний статус; • зростаючий попит на криптовалюти; • несхильність до ризику інфляції; • децентралізація валюти та відсутність головного регулятора дає можливість встановлення курсу відповідно до умов і факторів впливу на нього з боку ринку; • нові можливості у сфері мікроплатежів; • можливість і зручність здійснювати платежі у благодійні фонди.	• Абсолютна анонімність; • високі ризики для інвестування у даний об'єкт через перманентні флуктації курсу; • низький рівень безпеки операцій; • відсутність гарантій; • правова неврегульованість; • можливості для ухилення від оподаткування; • розгортання спекулятивних та шахрайських операцій через створення фінансової піраміди, отримання відсотків; • можливість формування нових схем відмивання грошей; • неможливість скасування трасакцій.

*Складено автором на основі [2].

Фундаментальні основи Zcash розробив у 2013 р. Метью Грін – керівник кафедри прикладної криптографії Університету Джонса Хопкінса. У розробці пізніше взяли участь криптографи Елі Бен-Сассон з Ізраїльського технологічного інституту, а також група дослідників з Массачусетського технологічного інституту і Університету Тель-Авіва [3].

В системі Zcash програмне забезпечення видає ряд випадкових значень, які приймаються у якості вихідних параметрів. Воно також генерує фрагменти криптографічного ключа, які разом можуть використовуватися для генерації нових монет Zcash. На церемонії запуску продемонстрували як відбувається створення і поширення цих фрагментів криптографічного ключа таким чином, що сам ключ ніколи не втілюється в реальності повністю [3].

Експерти переконані, що математично гарантована анонімність – головна перевага Zcash перед усіма іншими криптовалютами.

Першочерговим завданням для правоохоронних органів, які займаються фінансовими злочинами, є повернення незаконно одержаних активів та перекриття злочинцям доступу до доходів від їхньої злочинної діяльності. Проте для повернення незаконно отриманих активів їх необхідно спочатку розшукати. Під фінансовим розшуком активів мається на увазі процес, в якому слідчий виявляє, відстежує та встановлює місце перебування доходів від злочинної діяльності. Традиційне розслідування з розшуку активів має три стратегічних напрямки:

– встановлення місця перебування активів;

– ідентифікація їх як незаконної діяльності, що дасть можливість отримати постанови суду про їх заморожування та конфіскацію;

– доведення фактів вчинення відповідних злочинів [4].

В цьому контексті зазначимо, що динаміка зростання криптовалют дозволяє не тільки зберігати та убезпечувати свої заощадження від інфляції в країнах із нестабільною національною валютою, а й забезпечує перспективи для примноження свого капіталу. Це спричиняє зростання попиту на криптовалюту серед усіх верств населення, у тому числі серед хакерів, наркоторговців, організаторів схем відмивання коштів та інших зловмисників, що у сучасних умовах стає викликом та загрозою національним інтересам. Особливо небезпечною є можливість використання схем фінансування російських диверсантів на території за допомогою криптовалюти [4].

Серед технологій та схем у сфері криптовалют популярності набуває анонімна версія – даркнет. Терміном «даркнет» позначають сукупність веб-сайтів, видимих публічно, які мають прихований IP-адрес сервера, на якому вони розміщуються. Такі сайти можуть відвідувати всі веб-користувачі, але з'ясувати, хто є їх автором, – дуже складно. У той же час на подібні сайти неможливо потрапити, використовуючи популярні пошукові системи.

Практично всі сайти, що знаходяться в так званому даркнеті, приховують свою приналежність, використовуючи інструмент шифрування Tor. Технологія Tor дозволяє користувачам зберігати свою анонімність в Інтернеті при відвідуванні сайтів, веденні блогів, відправленні повідомлень [5].

За допомогою технології Tor здійснюється приховування особистих даних і місця розташування. У випадку, коли в управлінні мережі Tor знаходиться вебсайт, ефект спостерігається той же, що і в ситуації з кінцевим користувачем. Для того, щоб відвідати сайт в даркнеті, який використовує інструмент шифрування Tor, веб-користувач повинен також використовувати Tor.

Чорні ринки даркнету продають свої товари і послуги анонімним клієнтам, які часто розплачуються біткоїнами. Один з найбільших маркетів даркнету – Alphabay Market. В даркнеті доступні різні види наркотичних препаратів – близько 70%. Також можна купити акаунти в соцмережах, персональну інформацію і сканування паспортів, різні документи – від номерів паспорту до водійських прав. Розповсюдженим товаром у даркнеті є скановані копії кредитних карт, які використовуються для картингу – викрадення коштів із цих карт. Широкого розповсюдження здобуває даркнет і в Україні, де є десятки сайтів з можливістю анонімно придбати нелегальні товари [5].

Найбільшим ризиком популяризації криптовалюти для України є легкість легалізації коштів, отриманих злочинним шляхом. Відсутність зв'язку між рахунками у віртуальних валютах і реальними людьми в поєднанні з можливістю володіти необмеженою кількістю рахунків зумовлює сприятливе середовище для створення нових складних моделей, спрямованих на приховування незаконного походження коштів.

Для прикладу розглянемо той факт, що будь-який користувач мережі біткоїн може створити будь-яку кількість адрес без ідентифікації. Транзакції між двома адресами, обидва з яких контролюються одною і тою ж людиною, не відрізняються від операцій, в яких різні люди контролюють ці адреси. Таким чином, теоретично зловмисники можуть провести, наприклад, 100 000 Bitcoin-транзакцій між адресами, які ними ж і контролюються, перед тим, як перетворити біткоїн в іншу форму. Відновлення такого ланцюга операцій, особливо якщо це робиться вручну, зайняло б, як мінімум, дуже багато часу, якби взагалі виявилося можливим. Такий прийом може бути частиною складної схеми з відмивання грошей з використанням декількох осіб, віртуальних валют. Так само, як і первинна торгівля віртуальними валютами, яка відбувається з адміністраторами або біржами віртуальних валют, вторинна торгівля віртуальними валютами, як, наприклад, при використанні Інтернет-аукціонів або інших торгових майданчиків, також створює сприятливі можливості для збільшення складності проведення розслідування транзакцій [6].

У випадку з централізованими віртуальними валютами адміністратор має можливість ввести обмеження щодо максимальної суми операцій. Однак такі заходи, як правило, спрямовані на попередження потенційного шахрайства всередині системи. Аналогічним чином біржі віртуальних валют можуть встановлювати обмеження щодо суми для нових рахунків. Будь-які суми без обмежень або контролю можуть бути переведені за допомогою децентралізованих віртуальних валют. У випадку з біткоїн сума угоди ніяк не впливає на алгоритм проведення транзакції. До тих пір, поки власник Bitcoin-адреси може підтвердити свої права власності на певну кількість біткоїн, він має можливість перевести на один або кілька Bitcoin-адрес, незалежно від кількості переданих біткоїн.

Анонімність, велика кількість місць, в яких приймається оплата за допомогою нових способів платежів, можливість здійснення різних операцій, а також можливість зняття готівки через банкомати є одними з головних чинників, що підвищують привабливість нових способів платежів для злочинних елементів, які займаються відмиванням грошей. Анонімність може бути забезпечена шляхом використання анонімних продуктів. Крім того, анонімність може бути досягнута за допомогою незаконного використання персональних продуктів і особистих даних (тобто шляхом відходу від перевірки особистості за допомогою підроблених або вкрадених посвідчень особи або за рахунок використання фіктивних або підставних осіб, і т. д .) [3].

Адміністратори і біржі віртуальних валют регулюються лише в деяких юрисдикціях. Прогалини у сфері контролю з боку державного регулятора адміністраторів і бірж віртуальних валют – це ключовий фактор ризику як для обслуговуючих даний бізнес фінансових установ, так і для юрисдикцій поряд з відсутністю або недостатнім режимом санкцій.

Однією з труднощів в частині ліцензування та нагляду є те, що юрисдикція реєстрації та юрисдикція, де здійснюється основна діяльність, не збігаються, біржа або адміністратор може бути зареєстрований як компанія міжнародного бізнесу (офшор) і при цьому використовувати банківські рахунки в інших країнах. У деяких випадках проблемою може стати відсутність спеціального законодавства для постачальників фінансових послуг. Більшість операцій з віртуальними валютами припускають мінімальний або не передбачають взагалі контакт клієнтів і адміністратора.

Після застережень з боку Групи з протидії легалізації злочинних доходів та фінансуванню тероризму (FATF) були опубліковані документи, що стосувалися загроз, пов'язаних з цифровою валютою, з точки зору її використання для фінансування злочинної діяльності. У квітні 2012 р. Федеральне бюро розслідувань США оприлюднило результати оцінки оперативної інформації під заголовком «Віртуальна валюта біткоїн: унікальні характеристики створюють нові виклики для стримування незаконної діяльності». Основні тези документу полягали в дослідженні феномену біткоїн та складнощах виявлення підозрілої діяльності, встановленні особи користувачів та отриманні документи про трансакції [3].

Злочинні організації вже використовували цифрову валюту для результативного відмивання доходів від своєї злочинної діяльності. Показовим прикладом був коста-риканський переказувач виплат під назвою «резерв свободи». Він свідомо приймав підозрілі депозити, конвертував їх у свою власну цифрову валюту (долари «резерву свободи»), після чого знову здійснював конвертацію в чисту валюту після процедури позбавлення коштів будь-яких ознак місця їхнього походження. Діяльність з відмивання грошей проводилась цілком анонімно. Проте службою фінансових розслідувань ця схема була виявлена, проте обсяг проведеної операції з відмивання грошей сягнув близько 6 млрд. дол. США [3].

Одним із методів є використання властивостей трансакцій для встановлення зв'язків. Протокол біткоїн переказує суми від одного користувача до іншого, не пересуваючи фактичні «монети». Особа має у власності біткоїн, якщо в Blockchain є трансакція, за якою гроші відправляються на адресу, яку ця особа контролює, маючи асоційований приватний ключ. Якщо подивитися на трансакцію в Blockchain, в ній будуть показані її вхідні дані (походження відправлених біткоїнів), її вартість, мітка часу (що раз і назавжди посвідчує момент здійснення трансакції), а також її вихідні дані (адреса призначення, відправлених біткоїнів).

Наступним дієвим методом розслідування є використання обмінних центрів для збирання інформації.

В минулому обмінні структури працювали в спосіб, що був притаманний дикому заходу, майже або й зовсім не маючи будь-яких зобов'язань, проте тепер від них вимагається реалізація контрольних заходів «знай свого клієнта» (KYC), а в багатьох країнах – ще й реєстрація як структур, що займаються переказом грошей. За наявності таких вимог можна припускати, що центри обміну цифрової валюти можуть стати корисними партнерами в розслідуваннях, що проводять правоохоронні органи. З їхньою допомогою слідчі та прокурори можуть отримувати доступ до більшого обсягу інформації про сторони, що здійснюють перекази, аніж тільки мати їхні адреси, наприклад:

– контактна інформація: ім'я та прізвище, дата народження, адреса, телефон, адреса електронної пошти, копія документа, що посвідчує особу, або паспорту;

– інформація користувача: історія залишків на рахунку, login (місце, час та IP-адреса);

– фінансова інформація: номери банківського рахунку або кредитних карток, що використовувалися для поповнення рахунку або зняття коштів [4].

На своїй сторінці «угода з користувачем» обмінні центри біткоїн згадують про правила KYC, яких вони дотримуються, та повідомляють користувачів про те, що від них може вимагатися розкриття відомостей про їхніх клієнтів, а також «відмова в здійсненні або скасування будь-якої незавершеної трансакції з біткоїнами у відповідності до вимог закону або за судовою постановою, наказом або за іншим обов'язковим для виконання державним документом» [6].

У квітні 2014 р. Базельський інститут управління організував практичний семінар «Відмивання грошей через віртуальну валюту: новий виклик», учасниками якого стали представники банківського сектору з кількох країн, що брали участь в розслідуванні «Шовкового шляху». На семінарі основна увага була приділена відповідям на два основних запитання, до яких привело зазначене розслідування: як розшукати докази, і яким чином працювати із закодованими доказами [4].

Міжнародне співробітництво у сфері запобігання злочинам, пов'язаними з використанням криптовалют, має принципове значення у розслідуваннях, що охоплює декілька юрисдикцій, завдяки чому відбувається вчасний обмін оперативною інформацією. Отже, орган, що звертається із запитом, отримує можливість доступу до конкретних законодавчих вимог країни, що отримує такий запит. У цьому

відношенні для отримання судових рішень про заморожування активів та арешт даних може бути корисною конвенція ради Європи про кіберзлочинність.

Особливу увагу слід приділяти способу зберігання таких матеріалів згідно з вимогами експертизи для того, щоб вони не втратили свою доказову вагу та не дали приводів для закидів щодо їх підробки або щодо незаконного порядку їх отримання, що може зашкодити провадженню в справі.

Висновки. Підсумовуючи викладений матеріал, можна зробити такі висновки і узагальнення:

– по-перше, в результаті дисбалансів та асиметричності грошових потоків наслідок перманентних фінансових криз виникла потреба створення нових валют, які б вирізнялися децентралізацією та самостійністю.

По-друге, аргументовано доведено, що вивченню феномену Blockchain доцільно приділяти всебічну увагу, оскільки це дасть змогу запобігати злочинним технологіям і схемам пов'язаних з використанням цифрових валют. В даному контексті особливу увагу варто приділяти навчанню та підвищенню кваліфікації фахівців, держслужбовців та правоохоронних органів на основі співпраці з урядами інших країн та міжнародної правової допомоги.

По-третє, здійснення заходів забезпечення фінансових розслідувань, пов'язаних із пошуком та виявленням злочинних схем збагачення та розшуканих активів, вимагає їх необхідного збереження. У міжнародній практиці застосовують варіант обміну вилучених біткоїнів на звичайну валюту через волатильність та потенційне знецінювання вилучених активів.

Список використаних джерел

1. *Информаційний портал «Blockchaininfo» [Електронний ресурс]. – Режим доступу : https://blockchain.info/ru/charts/market-price.*
2. *Куцевол М. А. Поняття та економічна природа криптовалюти [Електронний ресурс] / М. А. Куцевол, О. А. Шевченко-Наумова. – Режим доступу : http://ir. kneu.edu.ua:8080/bitstream/2010/16391/1/79-85.pdf.*
3. *Поппер Н. Цифровое золото: невероятная история Биткойна // Поппер Н. – М. : ООО «И.Д. Вильямс», 2017. – 368 с.*
4. *Розшук незаконно отриманих активів [Електронний ресурс]. – Режим доступу : http://C:/Users/Admin/Desktop//160323_tracing_illegal_nslation_final_pdf.*
5. *Regulation of Bitcoin in Selected Jurisdictions. Report for Congress. The Law Library of Congress, Global Legal Research Center. 2014. LL File № 2014-010233. 25 p.*
6. *Bal A. How to Tax Bitcoin? // Handbook of Digital Currency. Singapore, 2015. Pp. 267–282.*

References

1. *Informaciynyi portal «Blockchaininfo» [Information portal «Blockchaininfo»] Retrieved from https://blockchain.info/ru/charts/market-price.*
2. *Kucevol, M.A. and Shevchenko-Naumova, O.A. (2010), Ponjattja ta ekonomichna pryroda krypto valjuty, available at: URL: http:// ir.kneu.edu.ua:8080/bitstream/2010/16391/1/79-85.pdf.*
3. *Popper N. Tsifrovoe zoloto: neveroyatnaya istoriya Bitkoyna [Digital Gold: The Untold Story of Bitcoin]. Moscow, 2016. 368 p.*
4. *Rozchuk nezakonno otrymanykh aktyviv (2015) [Search for illegally obtained assets]. Retrieved from http://C:/Users/Admin/Desktop//160323_tracing_illegal_nslation_final_pdf.*
5. *Regulation of Bitcoin in Selected Jurisdictions. Report for Congress. The Law Library of Congress, Global Legal Research Center. 2014. LL File No. 2014-010233. 25 p. (In Eng.).*
6. *Bal A. How to Tax Bitcoin? Handbook of Digital Currency. Singapore, 2015. Pp. 267–282. (In Eng.).*

Стаття надійшла до редакції 22.03.2018.