Шифр «Райські дива»

КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ГРОШЕЙ У ЗЛОЧИННІЙ ДІЯЛЬНОСТІ

ЗМІСТ

ВСТУП

Актуальність обраної теми дослідження зумовлена комплексом чинників економічного, технологічного та правового характеру. За сучасних умов використання електронних грошей набуває все більшого поширення. Адже завдяки їм переказування коштів можливе по всьому світу. Електронні гроші полегшують здійснення грошових операцій, адже це заощаджує час на проведення будь-яких транзакцій. Проте, аналіз використання електронних грошей та можливість їх залучення до злочинної діяльності, свідчить про необхідність детальної уваги до зазначеного явища з боку, як законодавців, так і правоохоронців, а також обумовлює необхідність створення нових підходів та технологій виявлення злочинів, в яких використовуються електронні гроші.

Поява криптовалюти, різновид якої, на сьогодні сягає більше тисячі найменувань, потребує детального вивчення для проведення аналізу, для того щоб забезпечити ефективне правове регулювання, а також для створення механізму контролю щодо протидії різним проявам злочинної діяльності. Децентралізація, анонімність та швидкість − найосновніші властивості електронних грошей, які полегшують злочинним організаціям здійснювати незаконні операції. Аналіз дослідження технології використання криптовалюти (особливо, найпоширенішої з неї − Bitcoin) у призмі злочинної діяльності, виявив недосконаліть законодавства та необхідність забезпечити спеціальними знаннями та технологіями правоохоронні органи для подальшого виявлення, попередження та розслідування злочинів, при вчиненні яких використовуються електронні гроші.

Об’єктом дослідження є злочинна діяльність, пов’язана з використанням електронних грошей.

Предметом дослідження є криміналістичний аналіз використання електронних грошей у злочинній діяльності.

Метою дослідження є визначення загальних особливостей технології застосування електронних грошей у фінансових процесах та можливостей використання електронних грошей у злочинній діяльності.

Відповідно до мети було поставлено наступні **завдання**:

- дослідити історію виникнення електронних грошей;
- визначити поняття та сутність криптовалюти як різновиду електронних грошей;
- проаналізувати способи та технології використання електронних грошей у злочинній діяльності;
- охарактеризувати особистість злочинців.

Методи дослідження. Методологічною основою дослідження є система загальнонаукових та спеціальних методів пізнання, а саме: діалектичний метод – для визначення об'єкта, предмета, мети та завдань дослідження; порівняльно-правовий – для визначення поняття та сутності електронних грошей і крипто валюти (підрозділ 1.1., 1.2); історико-правовий – при дослідженні розвитку окремих концепцій та поглядів при розкритті генезису поняття «електронні гроші», «криптовалюта» (підрозділ 1.1); формально-логічний – для аналізу чинного законодавства та окремих теоретичних криміналістичних положень (розділ 1,2).

Усі методи дослідження використовувалися в їх діалектичному взаємозв'язку, що забезпечило переконливість і достовірність наукових результатів.

Практичне значення та наукова новизна результатів полягає у тому, що сформульовані у роботі положення, пропозиції та висновки, спрямовані на покращення слідчої, оперативної практики щодо виявлення, попередження і розслідування злочинів, пов'язаних з використанням електронних грошей.

Деякі результати наукового дослідження оприлюднено на: Всеукраїнській науковій конференції «Верховенства права очима правників-початківців» (м. Одеса, 18 листопада 2017 р.).

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЕЛЕКТРОННИХ ГРОШЕЙ

1.1. Історія створення електронних грошей та їх використання

З розвитком мережі Інтернет почали з'являтися і електронні гроші. Історія виникнення електронних грошей безпосередньо пов'язана з розвитком комп'ютерних технологій та поширенням електронної комерції. Характеристика електронних грошей обумовлена формою носіїв інформації, характером емісії, способами розрахунків тощо.

У сучасному вигляді електронні гроші поділяються на дві основні категорії: електронні гроші карткового типу та електронні гроші програмного типу. Електронні гроші виникли та з початку набули поширення як гроші карткового типу. Сам термін «електронні гроші» стосувався сум, які відображалися на чипах карток традиційних платіжних систем. У порівнянні до карток з магнітною смугою, платіжні картки з чипом підвищували захист персональної інформації, зазначеної на картці, та надавали користувачам можливість здійснення трансакцій за відсутності їх авторизації з боку банку. Таким чином, із самого початку свого існування, електронні гроші карткового типу за своїми індивідуальними ознаками мали приналежність до певної платіжної системи, певного банку та були пов'язані з певним банківським рахунком.

Послідовність етапів розвитку електронних грошей починають свій розвиток із записів у комп'ютерній пам'яті банків, які передруковувалися із паперових носіїв. У минулому столітті за допомогою електронних імпульсів, які були наділені правом платіжного засобу, виникли цифрові гроші та електронні гаманці [6].

Історія електронних грошей почалась в 1918 році, коли Федеральний Резервний Банк США здійснив перший переказ через телеграф. Однак, донедавна цей спосіб взаєморозрахунків не користувався широкою популярністю.

Перший етап електронізації (1960-ті – кінець 1980-х років) полягав у переході на електронну основу оптових платежів. Він характеризувався появою клірингових розрахункових систем, автоматизованих розрахункових палат, а також широким використанням систем електронних трансфертів.

Починаючи з середини 1970-х років електронні трансферти (Electronic Funds Transfers – EFT) стали використовуватися у операціях міжбанківського клірингу.

Другий етап електронізації (з початку 1990-х років до теперішнього часу) полягає у переході на електронну основу роздрібних платежів. Він характеризується появою нових платіжних інструментів на базі електронного доступу до рахунків (access products) і електронних рахунків (e-money products) [1].

До речі, появу електронних грошей пов'язують з ім'ям Д. Чоума, нідерландським вченим, який в 1994 році вперше організував схему електронних грошей під назвою DigiCash, яка забезпечувала конфіденційність фінансових операцій та анонімність платежів. Проте, ця схема не була досить вдалою, але стала поштовхом для поширення значної кількості різноманітних електронних платіжних систем. З'явилося багато переваг у їх користуванні, але це призвело до відповідних ризиків, так як ними користувалися як кримінальні особи, так і кримінальні структури для полегшення легалізації доходів, здобутих злочинним шляхом та ін. Відсутність повного контролю з боку державних органів для здійснення різноманітного роду операцій у торгівлі, секторі послуг, може призвести до порушень законодавства, наприклад, ухилення від сплати податків.

Електронні гроші – це, по суті, електронний аналог готівкових грошей, які існують у вигляді електронних записів, наприклад, у віртуальних гаманцях в Інтернеті (аналог рахунку в банку, який використовується лише для операцій з електронними грошима). Це умовні знаки, які «прив'язані» до курсу однієї валюти (гривні, рубля, євро тощо) та існують лише у мережі і ніде більше. Сукупність віртуальних гаманців, у яких для здійснення платежів

використовуються електронні гроші, називається системою електронних грошей [5].

Отже, за допомогою електронних грошей можна здійснювати різні платежі на просторах Інтернет в режимі реального часу. Крім того, існує особливість таких грошей, яка полягає у тому, що функціонувати вони можуть лише на основі спеціального програмного забезпечення.

В Європі в офіційних документах вперше було приділено увагу електронним грошам у 1994 р. у звіті щодо електронних грошей Європейського валютного інституту. Зміст документу мав оглядовий характер та у ньому вперше розглядався феномен електронних грошей як інноваційного інструменту розрахунків. За висновками звіту, які носили рекомендаційний характер, передбачалось, що право на їх випуск має бути надано тільки банкам [10].

Швидкий розвиток електронних грошей призводить до шахрайства у вигляді зломів відповідних комп'ютерних програм, несанкціонованого перенесення прихованих обсягів електронних грошей за допомогою банківських переказів з рахунків одного банку до іншого, під контролем злочинців. Для забезпечення недоступності та відкритості інформації про здійснення транзакцій для злочинців, так і для державних органів, було введено криптовалюту.

Причиною появи на ринку альтернативної грошової продукції у вигляді криптовалюти можливо вважати, з одного боку забезпечення безпеки клієнтів від шахрайства, з іншого - прозорість грошових операцій в електронному вигляді для учасників торговельної або іншої угоди.

Ідею криптовалюти «b-money» описав у 1998 г. Вей Дай. Свої пропозиції також зробив Ник Сабо, пропонуючи використовувати крипто валюту під назвою Bitgold [9, с. 133].

На сьогодні існує сотні видів криптовалют, які володіють вагомими перевагами. Цікаве спостереження пов'язано з тим, що до криптовалюти вперше звернувся фінансовий, кримінальний та тіньовий бізнес.

Гроші стають віртуальною реальністю, яка створена штучно за допомогою електронних засобів. Електронні гроші “працюють” за такою схемою: зберігаються вони у вигляді файлів, або зашифрованих записів на диску електронної платіжної системи. Їх особливістю є миттєвість переказів, приватність емісії, низька собівартість трансакцій та порівняна безпека. В Інтернеті вони теж не є чимось предметним, це лише запис того, що певна сума грошових одиниць було зареєстровано на рахунку клієнта або знято з нього і переказано на рахунок клієнта – одержувача коштів. Використовувати електронні гроші можна також не відкриваючи рахунок у банку. Аналогічно, як і звичайні гроші, їх можна дарувати, позичати іншим користувачам системи, конвертувати, за них можна купувати товари та послуги на підключених до системи сайтах. Все це надало категорії грошей нової якості.

Таким чином, поява і поширення електронних грошей у певному розумінні – це нова ера їх еволюції, коли інформація перетворюється у субстанційну основу сучасної економічної реальності. Відповідно банківські технології стають потужною інформаційною системою, що органічно уписуються у нову економічну реальність, яку сьогодні все частіше характеризують, як “інформаційну економіку” [2].

1.2. Поняття та сутність криптовалюти як різновиду електронних грошей

На теперішній час криптовалюта відіграє досить вагому роль у системі грошових відносин. Встановити сутність і правову природу даного явища представляється важко, тому що чітко закріпленого у нормативних актах визначення криптовалюти немає. Криптовалюта має значний вплив на світовий ринок, враховуючи, що реакція державних органів на її існування є неоднозначною. У деяких країнах криптовалюта була прийнята і введена у обіг, тоді як в інших країнах зазначене явище викликало явне неприйняття і відторгнення.

Криптовалюта, за визначенням, є типом цифрової валюти на основі криптографії або процесом перетворення відкритого тексту у шифрований текст, що робить читабельний текст нерозбірливим [10].

Використання криптографії при передачі даних має чотири основні цілі:

1) Конфіденційність - інформація не може бути зрозумілою для тих, кому це було неминуче

2) Цілісність - забезпечення передачі інформації залишається незмінним.

3) Непідтвердження - відправник інформації не може заперечувати, що він відправив інформацію пізніше, за датою та часом.

4) Аутентифікація - відправник і одержувач мають можливість підтверджувати особистість один одного, а також походження та призначення інформації [21].

Криптовалюта заснована на математичних принципах децентралізованої конвертованої валюти, яка захищена за допомогою криптографічних методів, тобто використовує криптографію для створення розподіленої, децентралізованої і захищеної інформаційної економіки. У криптовалюті використовуються відкриті і закриті ключі для переказу валюти від одної (фізичної чи юридичної) особи іншій, і для переказу криптовалюти кожен раз потрібний криптографічний підпис.

Безпека, цілісність і актуальність реєстрів операцій з криптовалютою забезпечується мережею пов'язаних одна з одною осіб (так званих «Майнерів» (miners)), які захищають мережу в обмін на можливість отримання довільно розподілених комісійних зборів.

Були виявлені сотні варіацій криптовалют, більшість з яких пов'язані з Bitcoin, в якому використовується принцип «proof-of-work» («докази виконання роботи» - система, заснована на тому, що будь-яка операція вимагає певної кількості обчислень) для перевірки і підтвердження правильності операцій і ведення ланцюжка блоків. Хоча Bitcoin є першим працюючим криптографічним протоколом для крипто валюти. Зростає інтерес до розробки альтернативних, більш ефективних методів перевірки і підтвердження правильності операцій,

таких, як системи «proof-of-stake» («доказ володіння» - система, в якій нові монети генерується не за рахунок використання обчислювальних ресурсів, а за рахунок тривалості зберігання старіших монет») [3].

Віртуальна валюта - це форма нерегульованих цифрових грошей, яка не випускається або гарантується центральним банком, проте може виступати в якості засобу оплати.

Віртуальні валюти набули різних форм, починаючи з валюти в онлайн-ігрових середовищах та у соціальних мережах, а також у платіжних засобах, які приймаються в режимі офлайн або у реальному житті. На даний час все частіше використовуються віртуальні валюти як засіб для оплати товарів і послуг з роздрібними торговцями, ресторанами та розважальними закладами. Ці операції часто не несуть жодних податків або зборів.

Зовсім недавно віртуальна валюта "Bitcoin" встановила сценарій для нового покоління децентралізованих однорівневих віртуальних валют. Віртуальні валюти можна придбати на платформі обміну за допомогою звичайної валюти. Потім їх переводять на персональний обліковий запис, відомий як "цифровий гаманець". За допомогою цього кошика споживачі можуть відправляти віртуальні валюти в Інтернеті будь-кому, хто бажає їх прийняти, або конвертувати їх у звичайну валюту (наприклад, євро, фунт або долар) [18].

Bitcoin - це перша децентралізована P2P (від клієнта до клієнта) платіжна мережа, яка обслуговується її користувачами без центральних керівних органів та агентів. З точки зору користувачів Bitcoin − є аналогом готівки, однак, тільки для Інтернету [19], враховуючи, що їх максимальна кількість у світі обмежена до 21 мільйону.

Децентралізовані віртуальні валюти основані на математичних принципах піринговых віртуальних валют з відкритим початковим кодом, в результаті якого немає центрального адміністратора та відсутній контроль та нагляд. Хоча поряд з Bitcoin існують інші децентралізовані віртуальні валюти, він виступає найбільш яскравим прикладом серед них. За допомогою

пірингової мережі відбувається здійснення управління транзакціями. При цьому інформація про передачу права власності розповсюджується через мережу таким чином, щоб забезпечити безпеку цілісності її передачі, по закінченні короткого періоду часу [14].

Європейський суд у рішенні від 22.10.2015 визначив, що Bitcoin необхідно вважати валютою (засобом платежу), а не товаром. Це було обумовлено тим, що виникали певні труднощі щодо оподаткування криптолюти. Відповідне рішення встановило, що всі операції, пов'язані з обміном біткоїнів (bitcoin), будуть оподатковуватися так само, як і операції з традиційними валютами. Європейська судова практика по суті прирівняла криптовалюту до законного платіжного засобу, а обмін грошових коштів – «валютно-обмінною операцією» [10].

Розуміючи, що довіра між споживачами та фінансовою індустрією стрімко зменшується через збільшення витрат на посередництво та основні транзакції, Сатоши Накамото прагнув забезпечити безпечний спосіб оплати споживачам, який би втілював чотири цілі криптографії та дозволив їм почуватись більш безпечно. Ця нова електронна платіжна система, яка називається Bitcoin, буде мати транзакції на основі криптографічного доказу Secure Hash Algorithm 256 (SHA256) і буде побудована на основі мережі P2P[21].

Останніми роками фінансові платежі зазнали безпрецедентної хвилі технологічних новинок із розробкою нових електронних методів оплати. Криптовалюти, включаючи Bitcoin, забезпечують підґрунтя злочинцям для протиправних дій.

Віртуальні гроші найчастіше використовуються для оплати послуг мобільного зв’язку, доступу до Інтернету, а також здійснення покупок у просторі Інтернет. Засоби переказуються за допомогою електронних гаманців іншим користувачам або переводяться у готівку у різноманітній валюті тим чи іншим способом, який не врегульований діючим законодавством. Однією з галузей, яка представляє значну проблему для правоохоронних органів, є

неліцензовані (P2P) обмінники. Bitcoin та інші віртуальні валюти - це переважний спосіб оплати на темних («darknet») ринках. Як правило, для неліцензованих обмінників P2P, щоб отримати Bitcoin від продажу незаконних товарів і послуг на «darknet» ринках. Проблема полягає в тому, що в наслідок торгів на "darknet" ринках здійснюється перетворення віртуальної валюти у традиційну валюту. Щоб уникнути вимог до звітування, незаконні продавці звертаються до P2P обмінників або самі стають P2P обмінниками, щоб конвертувати віртуальну валюту у традиційну. Слідчі можуть ідентифікувати адресу Bitcoin гаманця обмінника та використовувати інструменти та методи аналізу Blockchain для відстеження транзакції Bitcoin. Bitcoin - це не що інше, як комп'ютерні файли, що містять дані, схожі на носій або текстовий файл. Bitcoin генеруються через процес, який називається "майнінг". У цьому процесі оператори, які використовують програмне забезпечення, що працює на спеціалізованому апараті, обробляє транзакції.

Отже, віртуальні валюти функціонують як метод обміну вартості. Bitcoin − найбільш прийнятна форма віртуальної валюти з поточною ринковою вартістю близько 38 мільярдів доларів. Протягом останніх декількох років багато компаній по всьому світу схвалили Bitcoin як альтернативний спосіб оплати. Оскільки ця віртуальна форма вартості продовжує набувати легітимності, методи їх експлуатації для злочинних цілей, також поширюватимуться. Так наприклад, в Японії та США, Bitcoin використовується як законний платіжний засіб. Використання Bitcoin здійснюється за допомогою анонімної транзакції, оскільки можна надсилати та отримувати Bitcoin, не розкриваючи жодної ідентифікованої інформації. Кожен користувач має публічну адресу, яка використовується для купівлі, продажу або передачі Bitcoin, і кожна транзакція, проведена Bitcoin, записується на загальнодоступну базу даних Blockchain. За допомогою псевдоанонімності, Bitcoin стає популярним способом купівлі та продажу незаконних товарів та послуг, що знаходяться, як в Інтернеті, так і поза його межами [25].

Злочинці, і зокрема кіберзлочинці, останнім часом виявили значні успіхи у користуванні Bitcoin, і як форму плати, використовували саме віртуальні валюти. Проте більш традиційні злочинні організації, які займаються легалізацією (відмиванням) великих розмірів грошей, все ще перебувають на ранніх етапах адаптації та вивчення Bitcoin та інших криптовалют, при цьому не використовують їх у широкому масштабі. Bitcoin забезпечує доступ індивідам для створення, передачі, відмивання та викрадення незаконних коштів анонімно. Хоча віртуальні валюти можуть розвиватися як інструмент фінансування злочинів і терористів. Цей ризик належним чином ще не реалізований [17].

Bitcoin, коли він поєднується зі сторонніми послугами, дозволяє користувачам міняти, купувати, продавати або приймати Bitcoin з будь-якої точки світу. Децентралізована функція Bitcoin унікальна серед віртуальних валют.

Bitcoin викликає низку ускладнень, пов'язаних з іншими віртуальними валютами, наприклад, таких як WebMoney, Paypal. До того ж додає унікальних складнощів для слідчих завдяки децентралізованій природі.

І ще одне зауваження. На відміну від традиційної готівки, електронні гроші у багатьох країнах до цих пір не підкріплені державою, в якості законного платіжного засобу. Зокрема, відсутня законодавча база щодо випуску, обігу та погашення електронних грошей. Відсутня прозорість операцій з електронними грошима. Очевидним є і невисокий рівень культури населення, високий рівень злочинності, пов'язаної з електронними грошима, відсутність гарантій погашення електронних грошей. Неприйнятні платежі за послуги електронного обігу з боку банків [4].

Україна входить у Топ-10 країн світу за кількістю користувачів Bitcoin. В Україні здійснює свою діяльність найбільше біткоін-агентство Kuna, одним з проектів якого є криптовалютна біржа. Тут функціонують також і великі девелоперські і дослідницькі компанії, наприклад, Distributed Lab. Застосування

децентралізованих технологій планується і частково реалізується на державному рівні: e - Vox, E - Ukraine.

Разом з тим в Україні також розвинуте криптовалютне співтовариство. При цьому варто зазначити, що до сих пір не вироблений підхід до регулювання криптовалютної діяльності та не визначений правовий статус цифрових валют [13].

Лист НБУ від 2014 року містить роз'яснення, в яких «віртуальна валюта/крипто валюта» Bitcoin розглядається як грошовий сурогат, який не має забезпечення реальною вартістю і не може використовуватися фізичними та юридичними особами на території України як засіб платежу, оскільки це суперечить нормам українського законодавства [12].

Незважаючи на це, Нацбанк вирішив випустити свою криптовалюту у 2017 р. Така форма електронних грошей здешевить еквайринг і може стати альтернативною картковим платежам. Згідно з презентацією Департаменту платіжних систем та інноваційного розвитку НБУ в четвертому кварталі 2017 р. Нацбанк збирається стати емітентом електронних грошей на базі технології Blockchain у рамках проекту НСП «Простір». Таким чином, упровадження і використання електронних грошей має розглядатись як перспектива розвитку рівня персональних банківських послуг та як найпоширеніший спосіб безготівкових розрахунків для дуже великої кількості людей, а виважена правова регламентація їх використання з боку держави є пріоритетним напрямом у їхньому становленні.

Крім того, під час використання "віртуальної валюти/криптовалюти" Bitcoin існує фактор підвищеного ризику, пов'язаного зокрема з анонімністю та децентралізованістю операції [8].

Оскільки Bitcoin не має централізованого управління, виявлення підозрілих дій, ідентифікації користувачів та отримання записів про транзакції є проблематичним для правоохоронних органів.

Розділ 2
КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ВИКОРИСТАННЯ ЕЛЕКТРОНИХ ГРОШЕЙ У ЗАБЕЗПЕЧЕННІ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ

2.1. Способи здійснення злочинної діяльності з використанням електронних грошей

Останнім часом з’являються великі ризики та небезпека у роботі з електронними грошима. Все частіше злочинці використовують електронні гроші у злочинній діяльності, зокрема такий вид електронної валюти як Bitcoin.

Перш за все треба визначити технологію роботи Bitcoin. Розглянемо Bitcoin як прихований дорогоцінний камінь, який потрібно видобути, щоб його вартість могла бути використаною. У цьому сенсі "видобуток" Bitcoin схожий на виявлення нових Bitcoin. Для відстеження транзакцій, які відбуваються з цією валютою, Bitcoin покладають на платіжну мережу від клієнта до клієнта. (Див. Додаток А). Аналіз практики використання зазначеної криптовалюти, дає можливість стверджувати, що кожна трансакція, повинна передаватися вузлом сусідів у мережі. Коли транзакція виконується користувачем, вузол, який отримує транзакцію, перевіряє автентичність транзакції особою, яка намагається здійснити трансфер, після чого вона намагається вирішити задачу (у термінах криптографії як інвертування хеш-функції). Після авторизації робиться доказ транзакції, який надсилається до інших вузлів у мережі. Цей процес перевірки винахідливості Bitcoin операції називають як видобуток або майнінг.

Завдяки численним академічним дослідженням, створили шифрування та програмні системи, які дозволяють розкривати незаконні дії з Bitcoin. Багато науковців та експертів у сфері комп'ютерних наук, економіки та судово-медичної науки співпрацюють з правоохоронними органами у пошуках та викритті злочинців (див. Додаток Б) [25].

З точки зору користувача, Bitcoin - це система електронних готівкових коштів. Будь-яка людина, яка має доступ до Інтернету та необхідну кількість пам'яті на своєму комп'ютері, може стати користувачем цієї електронної готівки. Першим кроком до початку використання Bitcoin є вибір гаманця на сайті "bitcoin.org" .

Гаманець може бути настільним (встановлений на комп'ютері), мобільним (встановлений на телефоні) та Інтернет-гаманцем.

Bitcoin-адреса створюється автоматично після створення гаманця. За допомогою цього гаманця користувач може здійснювати будь-які транзакції. Передача Bitcoin від одного користувача мережі до іншого здійснюється шляхом передачі Bitcoin з однієї адреси на іншу. Ця адреса забезпечує повну анонімність його власника.

Як це виглядає? Як комбінація цифр і букв, наприклад: "1D5wZqCjxNuPqfUN3RMFsxxxtqRBwiAeTZ". Кожен Bitcoin гаманець містить секретну інформацію про приватні ключі для всіх Bitcoin-адрес, яка належить конкретному користувачеві, тому можна здійснювати транзакції, якщо є приватний ключ із Bitcoin-адреси, призначеної для транзакції [20].

Blockchain — це децентралізована система зберігання даних або цифровий реєстр транзакцій. Розподілена структура даних, яка складається з послідовності блоків, в якій кожний блок містить хеш попереднього блоку, утворюючи, як наслідок, ланцюг блоків. Перший блок у ланцюжку розглядають як окремий випадок, оскільки в нього відсутній попередній блок. Blockchain працює як розподілена база даних, яка здійснює облік усіх операцій у мережі. Операції мають відзначку часу і зберігаються у блоках, де кожен блок ідентифікується своїм криптографічним хешем. Blockchain повністю зберігається у кожному вузлі мережі. Для роботи Blockchain не потрібно довіри між вузлами мережі, оскільки будь-який вузол може самостійно перевірити, чи збігається його копія бази з копіями, які зберігаються в інших вузлах [16].

Проводячи аналіз на рівні традиційних банківських моделях, останні досягли рівня конфіденційності, обмежуючи доступ до інформації сторонам і

довіреним сторонам. Необхідність публічно оголошувати всі транзакції перешкоджає цьому методу, але конфіденційність все ще може бути збережена, порушуючи потік інформації в іншому місці: зберігаючи відкриті ключі анонімно. Можна публічно побачити, що хтось надсилає суму іншому, але без інформації, яка зв'язує транзакцію з ким-небудь При кожній транзакції повинні використовуватися нові ключі, щоб зберегти їх від прив'язки до загального власника. Адже існує ризик, при якому можна викрити інші транзакції, які належать одному і тому ж власнику [24].

Дослідивши поняття та технологію використання Bitcoin у звичайному обігу, необхідно зазначити, що будучи віртуальною валютою, яка найбільш часто використовується в Інтернеті, виникає багато ризиків щодо її використання у злочинній діяльності.

Розглядаючи найбільш поширені простори використання Bitcoin у злочинній діяльності, можна виділити Mixers, Deep web, Silk Road.

1. Mixers, метод (простір) полягає у змішуванні грошей однієї особи з грошима іншої особи, що ускладнює процес впізнання походження грошей, так як вони змішані. Цей процес полягає у відправленні грошей анонімному сервісу. Пізніше така ж сума повертається, але вже змішана з Bitcoin від інших осіб. Таким чином, історія транзакцій будь-якого клієнта приховується, за допомогою Blockchain. Такий метод (простір) може використовуватися злочинцями наприклад при легалізації доходів, одержаних злочинним шляхом, адже за допомогою міксера можна уникати виявлення злочинних доходів.

2. Deep Web - це простір Інтернету, у тому числі інформація, яка недоступна в інших пошукових системах, таких як Google, Yahoo та ін. Не всі її дані є незаконними, також можуть бути дані про цензуру з урядів та корпорацій. Деякі нелегальні матеріали, які можна отримати тут, це: конфіденційні урядові файли, інформація про можливість купівлі та продажу наркотиків, зброї, виконавців для вбивств та багато іншого [23].

3. Silk Road є найбільший електронний чорний ринок у мережі Інтернет. Це почалося у лютому 2011 року, на даний час сайт вже не працює. Він був

створений з метою нелегальної торгівлі в усьому світі продуктами, ліками, та іншими товарами та послугами. Покупець направляв гроші на ринковий ринок, тут він зберігався, доки замовлення не досягне призначення поштою. Коли покупець отримував замовлення, то гроші переходили продавцеві. Даний ресурс являв собою анонімний торговельний Інтернет-майданчик, який знаходився в зоні анонімної мережі «Tor». Silk Road та був закритий 11 жовтня 2013 року після затримання його засновника Росса Ульбрихта. Результати показали, що Росс Ульбріхт отримав прибуток у розмірі 18 мільйонів доларів, майже 10% грошей було незаконними, від 1,5 мільйона транзакцій. Протягом усієї операції Bitcoin були конфісковані на суму 3,6 мільйонів доларів. Дана особа отримала обвинувачення у наркоторгівлі, хакерских атаках та задіянні у відмиванні грошей. Слід зазначити, що затримати власника Інтернет-магазину вдалося лише виявивши його посилку з дев'ятьма підробленими документами, які Ульбріхт планував використати з метою оренди серверів для Silk Road. Суд присудив йому монетарний штраф у розмірі 183 мільйонів доларів, а також два роки позбавлення волі [23].

Наводячи приклад щодо неправомірного використання електронних грошей, розглянемо схему, яка здійснюється на території України у термін із 2014 року і до тепер. Шляхом використання підроблених карток співучасникам вдалося придбати подарункові сертифікати торговельних мереж на суму не менш ніж 3 млн 762 тис. 501 Злочинна схема заволодіння грошовими коштами пов'язана з платіжними картками третіх осіб. Зокрема, маючи знання у сфері інформаційних технологій, затримана особа підшукала в мережі Інтернет сайт, на якому здійснювався продаж ідентифікаційних даних, так званих дампів, які були незаконно зчитані з магнітних смуг платіжних карток користувачів на території США. Таким чином дублікати могли бути використані без ризику блокування лише на території США. Затримана особа залучила співучасників для реалізації цієї схеми та організувала їх виїзд до США за рахунок залучення наявних там родинних зв'язків.

Після прибуття до США співучасники мали придбати обладнання, необхідне для створення дублікатів платіжних карток (пристрій для запису магнітних смуг, а також заготовки з магнітними стрічками), придбати дампи на сайті і виготовити необхідну кількість дублікатів. Потім вони мали використовувати зазначені підроблені картки для купівлі у роздрібних торговельних мережах подарункових сертифікатів відомих Інтернет-магазинів (Amazon, Ebay, Apple Store, iTunes та ін.), які могли бути використані замість грошей для купівлі товарів у зазначених магазинах.

Після купівлі достатньої кількості подарункових сертифікатів співучасники мали стерти захисне покриття на секретних кодах, сфотографувати зазначені сертифікати з відкритими секретними кодами та переслати зображення затриманій особі за допомогою електронної пошти для збуту іншим особам в обмін на сурогатні гроші, так звану криптовалюту Bitcoin. Це давало змогу здійснювати такі операції без розкриття реальних даних контрагентів із затриманою особою. Потім отримані Bitcoin обмінювалися на готівку у гривні або доларах США [11].

Розслідування злочинів та виявлення злочинної діяльності з використанням електронних грошей є досить важкою справою для правоохоронних органів. Натомість, у Інтерполі є відділ, який спеціалізується на злочинах, вчинених за допомогою використання віртуальних монет чи грошей, таких як Bitcoin. Існує спеціальна цифрова система, що забезпечує втручання поліції разом із фахівцями у цифрових зразках. Хоча дослідження щодо цієї нової технології все ще проводяться, деякі компанії та фінансові установи планують використовувати їх, інші вже застосували їх [23].

Всебічно продумана модель, забезпечує послідовність якісного розкриття етапів розслідування. Наприклад, модель, випущена DFRWS 2001, містить шість ключових етапів: ідентифікація, підготовка, збір, огляд, аналіз, презентація, збереження. Хоча ідентифікація та збереження є невід'ємними етапами моделі, основна увага цих досліджень зосереджується на етапах збору,

аналізу оскільки вони стосуються криміналістичних доказів для розкриття злочинів [23].

Отже, електронні гроші використовуються злочинними групами для здійснення різноманітних злочинних операцій. Варто зауважити, що саме децентралізовані електронні гроші мають успіх, адже вони не залежать ні від центральних органів держави, ні від фінансових установ, до того ж не існує стійкого правового регулювання. З іншого боку електронні гроші мають певні труднощі у функціонуванні. Процес транзакцій стає складним через розвиток нових технологій, і багато людей про це не знають. Це виступає перевагою для злочинців, і навпаки виступає труднощами для правоохоронної діяльності у процесі відстеження незаконних дій.

2.2. Характеристика особи злочинців

Надзвичайно швидкий розвиток інформаційних та комп'ютерних технологій останнім часом призводить до стрімкого розвитку злочинності, тому особливої актуальності сьогодні набувають питання протидії (виявлення, попередження та розслідування). Попередження злочинності базується на заходах, спрямованих на зниження ризику вчинення таких злочинів та нейтралізацію шкідливих наслідків для суспільства та приватного сектору.

З використанням електронних платіжних систем можуть бути здійснені наступні види злочинів: легалізація (відмивання) грошових коштів, отриманих злочинним шляхом, шахрайство, незаконне отримання кредиту, купівля незаконних товарів, крадіжка т.ін. Кількість таких злочинів зростає, змінюється їх якісний склад, що свідчить про значущість і про суспільну небезпеку. До того ж, електронні гроші можуть виступати засобом забезпечення злочинної діяльності

У криміналістичному аспекті важливого значення набуває дослідження умов формування особи: її схильності до порушення закону, особливостей характеру, професійні навики. Це зумовлює необхідність вивчення слідчим

навіть у загальних рисах особливостей життя злочинця, заняття певним видом діяльності.

Для осіб, що використовують електронні гроші, зокрема, криптовалюту, у злочинній діяльності, ризик бути виявленими значно зменшується через неузгодженість у діях правоохоронних органів різних країн, відсутність належної правової бази для протидії злочину. Тому встановлення причетності осіб до вчинення злочинів та притягнення їх до відповідальності залишається проблемою.

Безумовно найнебезпечнішу групу складають саме професіональні комп'ютерні злочинці, адже володіючи знаннями в області новітніх технологій без перешкод здійснюються найскладніші транзакції з електронними грошима. Адже вони прекрасно володіють програмуванням, що дозволяє маскувати усі їх дії. Тим самим ускладнюється їх виявлення для правоохоронних органів.

Більшості з них властиві порівняно високий рівень освіченості, швидка адаптація до нових змін у технологіях, забезпеченість професійною якісною технікою та ін. Здійснення злочинів у цій сфері вимагає від учасників певних знань, навиків і спеціальної підготовки. Найбільшу небезпеку і складність виявлення, розкриття та розслідування являють собою злочини, вчинені групою осіб, у складі яких присутні фахівці, які володіють спеціальними знаннями у сфері негласного отримання та захисту комп'ютерної інформації [15, с. 201].

Крім того, слід віднести висококваліфікованих фахівців з вищою математичною, економічною освітою, що входять до організованих злочинних групи і організацій, для яких характерні мобільність, фінансова освіченість, аналітичні навичку використання у злочинній діяльності фінансового ринку, мають право здійснювати фінансові операції.

Проте, вивчаючи технологію використання та здійснення операцій з криптовалютою, а саме Bitcoin, можна зробити висновок, що робота з однорівневою піринговою системою не є складною. Тобто, кожна особа, яка у змозі приділити увагу для вивчення технології блокчейн, зможе розробляти певні транзакції, які не будуть правомірними. Великий ризик, того, що майже

кожна людина зможе за допомогою криптовалюти легалізувати доходи, одержані незаконним шляхом.

Отже, такою діяльністю займаються, як особи з певним обсягом спеціальних знань, високоосвічені особи, звичайні громадяни, так і службові особи.

Не дивлячись на те, що Bitcoin був створений для підвищення довіри при здійсненні купівлі-продажі послуг у мережі Інтернет, з урахуванням того, що ці послуги можуть бути здійснені як на території одного міста, так і на території різних континентів (держав). Недоліком є неправомірне використання Bitcoin, та поява реальних схем легалізації (відмивання) тіньового капіталу, шахрайств, купівлі заборонених товарів та послуг за його допомогою. Користуючись властивостями криптовалюти, а саме гарантованістю що, клієнти залишаються анонімними, а також непідконтрольністю з боку центральних органів, злочинці та злочинні групи почали здійснювати операції, які дозволяють переводити нечисленні суми з одного рахунку на інший,. Зазначене можливо завдяки використанню криптовалюти у великих розмірах, що не передбачено звичайними фінансовими або банківськими операціями.

До того ж, криптовалюта використовується на різноманітних сайтах, які створені організованими злочинними групами, наприклад сайти дитячої порнографії, сайти для збуту наркотиків. Також небезпечними зонами використання електронних грошей, у тому числі і криптовалюти є зони проведення бойових дій, вчинення терористичних актів, де у зв’язку із політичною, економічною нестабільністю існує обіг коштів, здобутих від різних злочинних дій (наприклад, було здійснено багато транзакцій для купівлі зброї, за допомогою криптовалюти (Bitcoin) у східно-азіатських країнах). Також є інформація, що терористичні організації, такі як Daesh (також відома як ісламська держава Іраку та Сирії або ISIS), зацікавлені у використанні віртуальних валют, але повідомлення про те, що терористи активно використовують їх, як правило, не підтверджені [21].

Отже, проводити будь-які операції з електронними грошима можуть особи з певним обсягом спеціальних знань, фінансів, достатнім освітнім та професійним рівнем.

ВИСНОВОК

Незважаючи на відсутність на сьогодні загальноприйнятного визначення криптовалюти спостерігається досить широке та вичерпне розуміння його суті та способів його вчинення, а також загроз та ризиків, що дає можливість розробляти та запроваджувати заходи протидії злочинній діяльності.

Відсутність фізичного контакту з жертвою або представниками фінансової установи, а також анонімність, швидкість здійснення та невисока вартість злочину стали ключовими передумовами підвищення зацікавленості злочинців цифровими грошима, у тому числі криптовалютою. Особливістю електронних грошей є те, що при її використанні майже не залишається інформації про користувача, тобто забезпечена висока анонімність. Таким чином, необхідно адаптувати українське законодавство до міжнародних програм, що займаються протидією злочинної діяльності, яка здійснюється за допомогою електронних ресурсів, та спираючись на світовий досвід розробити законодавство, що регулюватиме діяльність та обіг електронних платіжних систем та валюти, враховуючи реалії. Потрібно зазначити, що на даний час розглядається проект Закону «Про обіг криптовалюти в Україні».

Для уникнення використання електронних грошей у незаконних цілях сподіваємося, що в майбутніх дослідженнях криптовалюта матиме законодавче регулювання, а також забезпечення належного рівня підготовки правоохоронних органів для вжиття ефективних заходів для попередження, своєчасного виявлення та протидії злочинній діяльності.

СПИСОК ВИКОРИСТАНОЇ ЛИТЕРАТУРИ

1. Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют [Електронний ресурс] // UNODC. – 2014. – Режим доступу до ресурсу: https://www.imolin.org/pdf/UNODC_VirtualCurrencies_final_RU_Print.pdf.

2. Богдан Івасів. Історія виникнення та перспективи розвитку електронних грошей / Івасів Богдан. // Світ фінансів. – 2008. – №2. – С. 157–160.

3. ВИРТУАЛЬНЫЕ ВАЛЮТЫ. Ключевые определения и потенциальные риски в сфере ПОД/ФТ [Електронний ресурс] // АНО «МУМЦФМ». – 2014. – Режим доступу до ресурсу: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf

4. Волошин В.С. К ВОПРОСУ О СВОЙСТВАХ ДЕНЕЖНЫХ АНАЛОГОВ [Електронний ресурс] / В.С.Волошин. – 2016. – Режим доступу до ресурсу: http://eir.pstu.edu/bitstream/handle/123456789/13473/%D1%81.4-10.pdf?sequence=1.

5. Дерев'янко Світлана. СУТНІСТЬ ЕЛЕКТРОННИХ ГРОШЕЙ ТА ОПЕРАЦІЙ З НИМИ / Світлана Дерев'янко. // Економічний дискурс. – 2014. – №2. – С. 268–272.

6. Іконнікова М.В. ЕЛЕКТРОННІ ГРОШІ В АСПЕКТІ ЕКОНОМІЧНОЇ ГЛОБАЛІЗАЦІЇ. РИНОК ЕЛЕКТРОННИХ ГРОШЕЙ УКРАЇНИ: ПЕРСПЕКТИВИ, ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ [Електронний ресурс] / М.В.Іконнікова. – 2012. – Режим доступу до ресурсу: http://zt.knteu.kiev.ua/files/2012/04(63)2012/4_12_23.pdf.

7. Кіт Я.Р. Світовий досвід та перспективи розвитку електронних грошей в Україні [Електронний ресурс] / Я.Р.Кіт. – 2015. – Режим доступу до ресурсу: http://libfor.com/index.php?newsid=2499.

8. Колесник В.М. ПРОБЛЕМИ СТАНОВЛЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЕЛЕКТРОННИХ ГРОШЕЙ В УКРАЇНІ [Електронний ресурс] / В.М.Колесник – 2017. – Режим доступу до ресурсу: http://global-national.in.ua/archive/17-2017/135.pdf.

9. Олиндер Н.В. Криминалистическая характеристика электронных платежных средств и систем. / Н.В.Олиндер. // НАУЧНЫЕ ТРУДЫ МГЮА. – 2015. – №22. – С. 128–139.

10. Плита А.І. КРИПТОВАЛЮТА: ЇЇ ПРАВОВИЙ РЕЖИМ, ПРОБЛЕМИ ЗАСТОСУВАННЯ [Електронний ресурс] / А.І. Плита. – 2017. – Режим доступу до ресурсу: http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_plyta_%D1%81ryptocurrency/.

11. Правоохоронці України виявили схему шахрайства та легалізації грошових коштів із використанням Bitcoin [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://ua.interfax.com.ua/news/general/441690.html.

12. Роз’яснення щодо правомірності використання в Україні "віртуальної валюти/криптовалюти" Bitcoin [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.bank.gov.ua/control/uk/publish/article?art_id=11879608.

13. Роль технології блокчейн і можливості використання криптовалют [Електронний ресурс] – Режим доступу до ресурсу: http://pkiforum.org.ua/wp-content/uploads/2017/10/Nevmergizkyi.pdf.

14. Сидоренко З.А. Створення Bitcoin гаманця із використанням технології Blockchain [Електронний ресурс] / З.А.Сидоренко // Київ. – 2017. – Режим доступу до ресурсу: http://cad.kpi.ua/attachments/093_2017d_Sydorenko.pdf.

15. Федоров М.І. Кіберзлочинність як результат глобалізації інформаційних процесів / М.І.Федоров. // Вісник Львівського Торговельно-економічного університету. – 2016. – №3. – С. 197–207.

16. Crosby M. Blockchain technology: Beyond bitcoin / M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman // Applied Innovation 2, 2016. – Pp. 6-10.

17. Carlisle David. Virtual Currencies and Financial Crime [Електронний ресурс] / David Carlisle // Royal United Services Institute – Режим доступу до ресурсу: https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf.

18. EBA warns consumers on virtual currencies [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies.

19. In Bitcoin information site [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: bitcoin.org/ru/faq#what-is-bitcoin.

20. INVESTIGATION OF MONEY LAUNDERING METHODS THROUGH CRYPTOCURRENCY [Електронний ресурс] // Journal of Theoretical and Applied Information Technology. – 2016. – Режим доступу до ресурсу: http://www.jatit.org/volumes/Vol83No2/11Vol83No2.pdf.

21. Michael Doran. A Forensic Look at Bitcoin Cryptocurrency [Електронний ресурс] / Michael Doran // the SANS Institute. – 2015. – Режим доступу до ресурсу: https://www.sans.org/reading-room/whitepapers/forensics/forensic-bitcoin-cryptocurrency-36437.

22. Report to the Council of the European Monetary Institute on Prepaid Cards. Working Group on EU Payment Systems. European Monetary Institute [Електронний ресурс] // Кочергин Д. Мировой опыт регулирования в сфере электронных денег – Режим доступу до ресурсу: http://dlib.eastview.com/browse/doc/7661158.

23. SARA RUIZ CABRERA. HOW DO YOU DO MONEY LAUNDERING THROUGH BITCOIN? [Електронний ресурс] / SARA RUIZ CABRERA. – 2015. – Режим доступу до ресурсу: http://repositori.uji.es/xmlui/bitstream/handle/10234/161136/TFG_2015_ruizS.pdf?sequence=1

24. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс] / Satoshi Nakamoto – Режим доступу до ресурсу: https://bitcoin.org/bitcoin.pdf.

25. Virtual Currency [Електронний ресурс] // HSI – Режим доступу до ресурсу:https://www.ice.gov/sites/default/files/documents/Report/2017/CSReport-13-2.pdf.

АНОТАЦІЯ

Актуальність даної теми зумовлена швидким та динамічним зростанням злочинності у економічній, комп'ютерній сферах. Тим самим вникає необхідність вивчення нових підходів та технологій виявлення злочинів, в яких використовуються електронні гроші. У дослідженні було проаналізовано технології використання криптовалюти (Bitcoin) у призмі злочинної діяльності, що показало необхідність зміни напрямів наукових досліджень і переорієнтації їх на вирішення проблем практики правоохоронних органів для забезпечення попередження, виявлення та розслідування проявів злочинної діяльності з використанням електронних грошей.

Метою дослідження є визначення загальних особливостей технології застосування електронних грошей у фінансових процесах та можливостей використання електронних грошей у злочинній діяльності.

Відповідно до мети було поставлено наступні **завдання**: дослідити історію виникнення електронних грошей; визначити поняття та сутність криптовалюти як різновиду електронних грошей; проаналізувати способи та технології використання електронних грошей у злочинній діяльності; охарактеризувати особистість злочинців.

Методи дослідження. Методологічною основою дослідження є система загальнонаукових та спеціальних методів пізнання, а саме: діалектичний метод – для визначення об'єкта, предмета, мети та завдань дослідження; порівняльно-правовий – для визначення поняття та сутності електронних грошей і крипто валюти (підрозділ 1.1., 1.2); історико-правовий – при дослідженні розвитку окремих концепцій та поглядів при розкритті генезису поняття «електронні гроші», «криптовалюта» (підрозділ 1.1); формально-логічний – для аналізу чинного законодавства та окремих теоретичних криміналістичних положень (розділ 1,2).

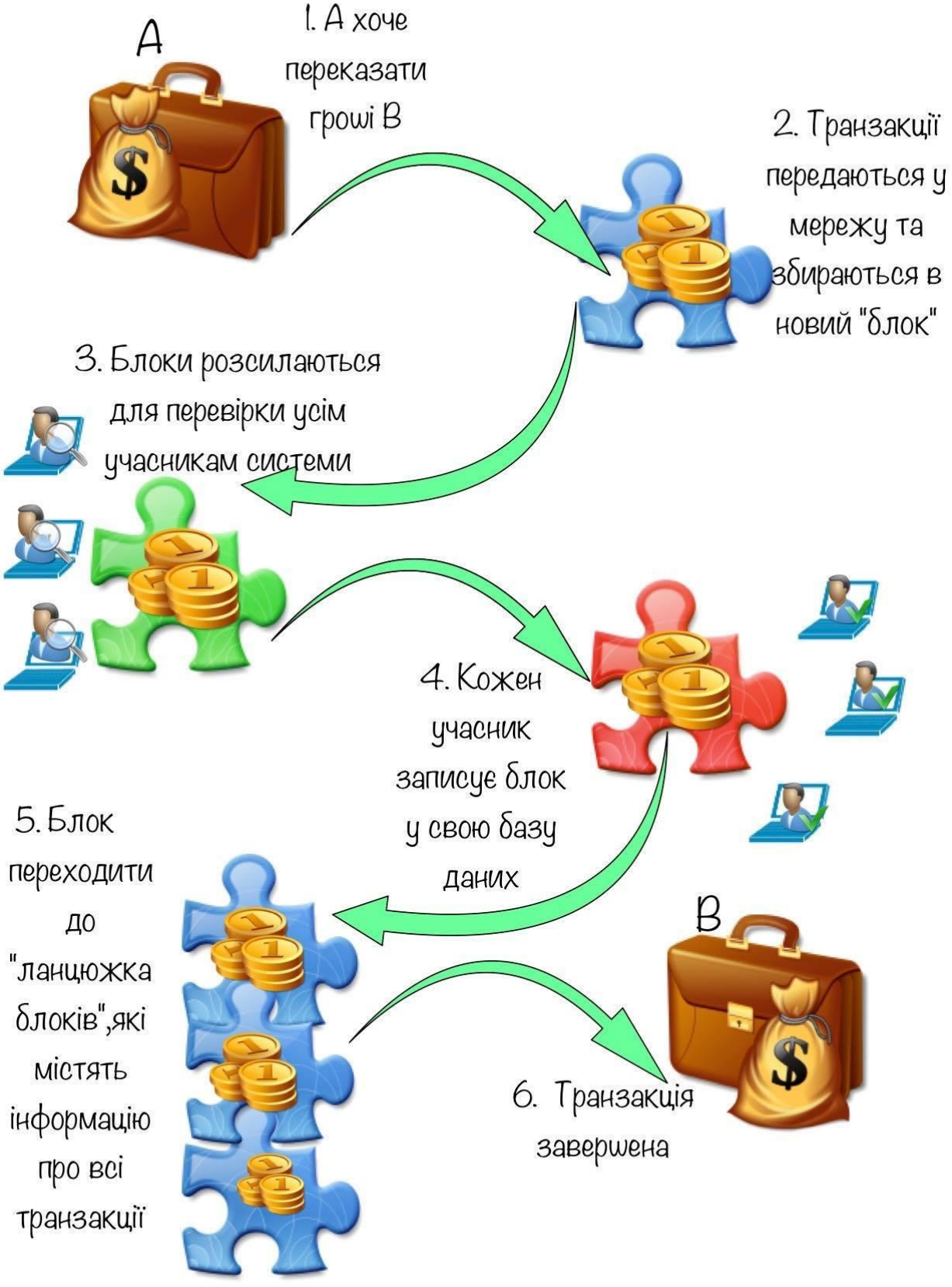
Практичне значення та наукова новизна результатів полягає у тому, що сформульовані у роботі положення, пропозиції та висновки, спрямовані на

покращення слідчої, оперативної практики щодо виявлення, попередження і розслідування злочинів, пов’язаних з використанням електронних грошей.

Деякі результати наукового дослідження оприлюднено на: Всеукраїнській науковій конференції «Верховенства права очима правників-початківців» (м. Одеса, 18 листопада 2017 р.).

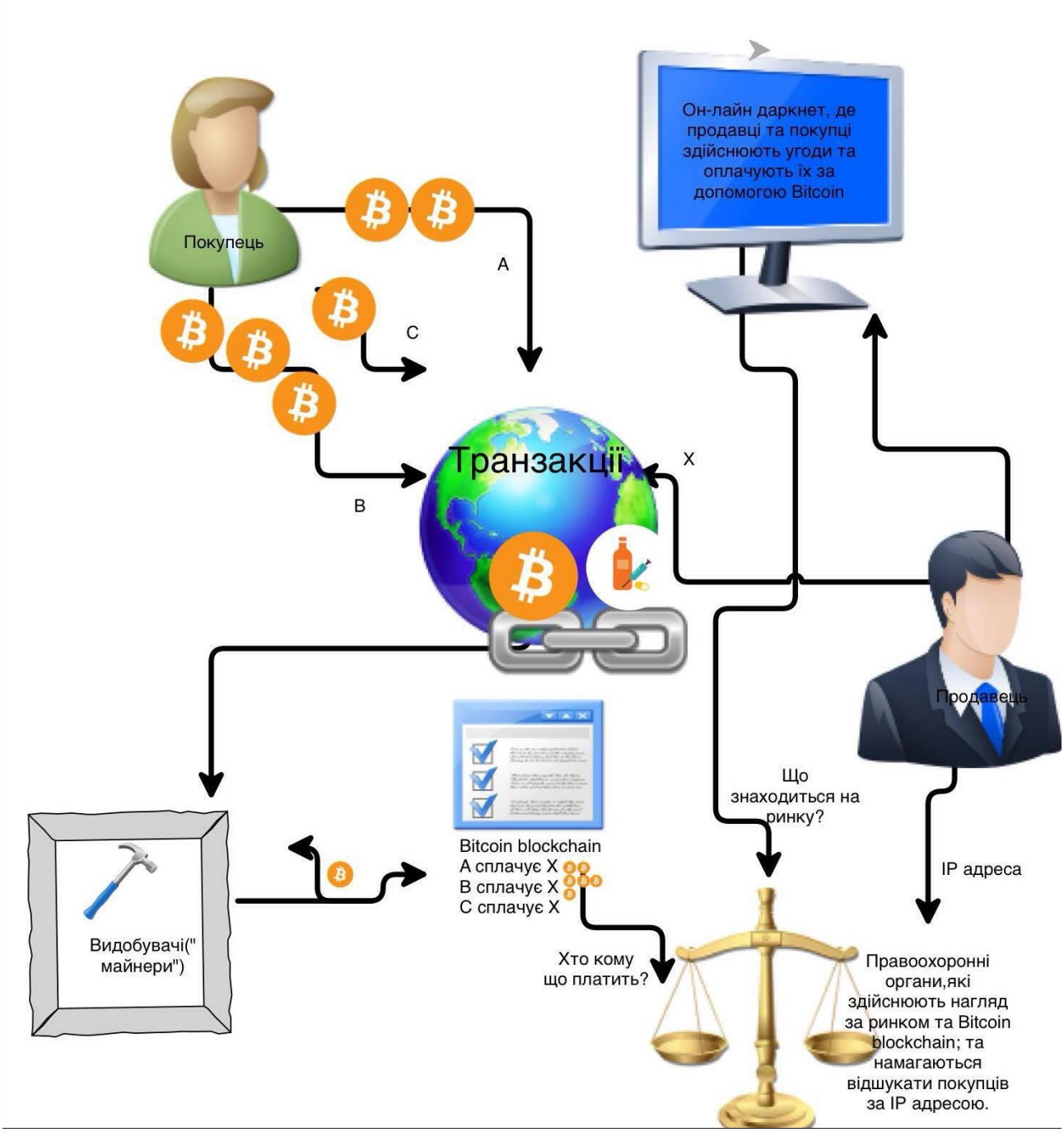
Структура даної роботи складається з вступу, двох розділів, кожен з яких включає в собі по два підрозділи, висновки, список використаної літератури, анотації та додатки.

Обсяг роботи складає 28 сторінок, кількість схем – 2, список використаних джерел – 25.


A
1. A хоче переказати гроші B
2. Транзакції передаються у мережу та збираються в новий "блок"
3. Блоки розсилаються для перевірки усім учасникам системи
4. Кожен учасник записує блок у свою базу даних
5. Блок переходити до "ланцюжка блоків",які містять інформацію про всі транзакції
B
6. Транзакція завершена

.

Додаток Б


Он-лайн даркнет, де продавці та покупці здійснюють угоди та оплачують їх за допомогою Bitcoin
Покупець
A
C
B
Транзакції
X
Продавець
Що знаходиться на ринку?
IP адреса
Bitcoin blockchain
A сплачує X
B сплачує X
C сплачує X
Видобувачі(" майнери")
Хто кому що платить?
Правоохоронні органи,які здійснюють нагляд за ринком та Bitcoin blockchain; та намагаються відшукати покупців за IP адресою.

VIRTUAL CURRENCIES AS A MEANS OF THE LAUNDERING OF CRIME PROCEEDS

The virtual currency has exploded in popularity in recent years. It has become increasingly used in criminal activities, such as money laundering obtained by criminals means.

The concept of money laundering implies an illegal activity, through which the criminal proceeds are legalized.

Virtual currency systems can be traded on the internet, are generally characterized by non-face-to-face customer relationships, and may permit anonymous funding or purchase (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

In this modern technology in the field of e-commerce have led to the emergence of new means of payment and settlement through a global network and its anonymous segments through various cryptocurrency, virtual currencies.

A FATF discussion paper on virtual currencies issued in June 2014 10 defines virtual currencies as ‘‘a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency” [4, c. 8].

For the purposes of this definition, a “digital representation” is a representation of something in the form of digital data. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system. The critical point of note in the use of the term “digital representation” is the fact that it is the digital data itself that is the virtual currency, not the medium on which the digital data is stored. Digital representations of virtual currency can be moved, copied or transferred to another storage medium, but the

value of the virtual currency remains inherent in the digital representation. Virtual currency is distinguished from fiat currency (a.k.a. “real currency”, “real money” or “national currency”), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country [1, c. 11].

The technology of such transfers is quite simple and convenient. A person is contacted at the branch of the system or its partner (it is necessary to have an identity document), which makes the necessary funds and completes the form indicating the name and the name of the recipient and the country where the transfer was sent. In the future, the operator will receive the number of the transfer, which must be notified to the recipient.

The recipient of the funds (with an identity document) applies to the branch of the system or its partner and fills in the form for the issuance of cash, indicating the transfer number, the sender's name and surname, the country of sending the transfer, the amount and currency of the transfer [2, c. 42].

Three main typologies related to the misuse of NPMs for money laundering and terrorist financing purposes were identified:

– Third party funding (including strawmen and nominees). For example, a young person, acting as a nominee, opened a digital currency account to enable him to receive the proceeds of Internet banking thefts from an offshore associate. He then attempted to redeem the value of the digital currency account by requesting the digital currency exchanger to provide him with postal money orders. In an effort to conceal his identity he informed the cash dealer that he had lost his passport and requested that the exchanger call a money service business and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted [3, c. 40].

– Exploitation of the non-face-to-face nature of many NPM accounts. As an example, two defendants were charged in 2009 with illegally accessing business computer systems via the Internet and fraudulently transferring funds from the

victims' bank accounts to prepaid cards. The defendants allegedly used stolen account logins and passwords to access victims' online personnel management accounts, which, among other things, allowed users to establish direct deposit of employee wages. The defendants allegedly directed employee wage payments to the hackers' prepaid card accounts. Over a period of 11 months, the defendants allegedly transferred USD 19 967.43 in illegally obtained funds [3, c. 42].

– Complicit NPM providers or their employees. For instance, in 2007, an Internet payment business based in the Isle of Man and publicly traded on the Alternative Investment Market ("AIM") of the London Stock Exchange — admitted to criminal wrongdoing and agreed to forfeit USD 136 million in criminal proceeds as part of an agreement to defer prosecution. The IPS business participated in a conspiracy to promote illegal (according to U.S. legislation) Internet gambling businesses and to operate an unlicensed money transmitting business [3, c. 49].

In this regard, there are a number of threats associated with virtual currencies. They are represented by such factors as fast and irrevocable transactions, anonymity, insufficient transaction data, complex transaction models, and what is most important is the absence of restrictions on the amount.

In addition, they cause difficulties in the investigation of their law enforcement agencies.

Investigative difficulties are expressed in a lack of knowledge about the existence and possibilities of virtual currencies.

There are limited possession of tools and methods for effective investigation of crimes committed through virtual currencies. Difficulties are also due to the necessary appropriate legislative framework to ensure the allowability of electronic evidence. Counteraction to illegal activities includes the full range of legal, technical, organizational and information activities.

Effective counteraction to legalization of proceeds obtained by criminal means is accomplished through the identification of financial transactions in time. International cooperation in the investigation of money laundering committed using virtual currencies is conditioned by the use of mechanisms for international

cooperation between investigative authorities and other agencies of the criminal justice system of the countries concerned. Cooperation at the international level is much more formalized than cooperation at the national level, in our opinion it needs to be ordered.

Sources

1. Базовое пособие по выявлению и расследованию отмывания преступных доходов, совершенного посредством виртуальных валют [Електронний ресурс] // UNODC. – 2014. – Режим доступу до ресурсу: http://crimescience.ru/wp-content/uploads/2015/08/%D0%9E%D1%82%D0%BC%D1%8B%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5-%D0%94%D0%B5%D0%BD%D0%B5%D0%B3_%D0%9F%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5.pdf.
2. Киберпреступность и отмывание денег [Електронний ресурс] // Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма. – 2014. – Режим доступу до ресурсу: http://www.eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014.pdf.
3. Новые способы платежей итоговый проект документа (30 сентября 2010 года) [Електронний ресурс] // XXII Пленарное заседание ФАТФ. – 2010. – Режим доступу до ресурсу: http://www.eurasiangroup.org/ru/news/Novye_sposoby_platezhey_2010.pdf.
4. Ключевые определения и потенциальные риски в сфере ПОД/ФТ [Електронний ресурс] // ОТЧЁТ ФАТФ. ВИРТУАЛЬНЫЕ ВАЛЮТЫ.FATF GAFI. – 2014. – Режим доступу до ресурсу: http://www.cbr.ru/today/anti_legalisation/fatf/Virtualnye_valyuty_FATF_2014.pdf.