Розшифровка криптозлочинів

Посібник для правоохоронних органів

ОБСЄ Організація з безпеки та співробітництва в Європі

Заява про відмову від відповідальності

Ця публікація підготовлена на основі оригінальних матеріалів, наданих автором. Ця публікація не підлягала редагуванню редакторами ОБСЄ. Висловлені в ній погляди залишаються відповідальністю автора, і не обов'язково відображають погляди ОБСЄ, місій або держав-учасниць.

ОБСЄ, її місії та держави-учасниці відмовляються від будь-якої відповідальності за будь-які наслідки, які можуть виникнути в результаті використання цієї публікації. У цій публікації не розглядаються питання про відповідальність, юридичну чи іншу, за дії чи бездіяльність з боку будь-якої особи. Згадка чи посилання на конкретні країни чи території у цій публікації не означає жодної позиції ОБСЄ щодо їхнього правового статусу, органів управління, установ, чи визначення їхніх кордонів.

Розшифровка криптозлочинів

Посібник для правоохоронних органів

ОБСЄ Організація з безпеки та співробітництва в Європі

Зміст

Акроніми, абревіатури та ключові терміни з поясненнями

5-та Директива про протидію відмиванню коштів (5th AML Directive)	Директива (ЄС) 2018/843 Європейського парламенту та Ради Європи від 30 травня 2018 року про внесення змін до Директиви (ЄС) 2015/849 про запобігання використанню фінансової системи для цілей відмивання грошей або фінансування тероризму, а також внесення змін до Директив 2009/138/ЕС та 2013/36/EU (текст з відповідністю вимогам ЄЕЗ). Ця директива додала до сфери її застосування криптоактиви. До 10 січня 2020 року держави-члени повинні впровадити необхідні закони та нормативні акти для дотримання цієї директиви.
ПВК (AML)	Боротьба з відмиванням грошей – це закони, нормативно-правові акти та процедури, покликані перешкодити злочинцям приховувати незаконно отримані кошти під виглядом законного доходу.
КАСП (CASP)	Постачальники послуг криптоактивів – організації, які пропонують послуги, пов'язані з криптоактивами. Ці послуги можуть охоплювати широкий спектр діяльності, включаючи, але не обмежуючись наступним: 1. Послуги обміну: забезпечення купівлі та продажу криптоактивів за фіатні гроші або інші криптоактиви. 2. Постачальники гаманців: пропонують кастодіальні або некастодіальні гаманці для зберігання, керування та переказу криптоактивів. 3. Послуги переказу: можливість переказу криптоактивів з однієї адреси або облікового запису на інший. 4. Фінансове консультування: надання консультацій щодо купівлі, продажу або зберігання криптоактивів. 5. Послуги зберігання: зберігання та захист криптоактивів від імені клієнтів. Постачальники послуг криптоактивів, див. с. 20.
РЄ (COE)	Рада Європи – міжнародна організація, яка займається відстоюванням прав людини, демократії та верховенства права в Європі.
ПФТ (CTF)	Протидія фінансуванню тероризму – стосується політики та дій щодо запобігання фінансуванню терористичної діяльності. Вона спрямована на виявлення та припинення потоку коштів як із законних, так і з незаконних джерел до угруповувань, які мають намір здійснити терористичні акти.
Токени ERC20 (ERC20 Tokens)	Токени ERC-20 (Ethereum Request for Comment 20) – реалізований 2015 року технічний стандарт, який використовується для створення і випуску смарт-контрактів у блокчейні Ethereum ("Ефір").
ЄС (EU)	Європейський Союз – політична та економічна організація 27 європейських країн, які розташовані на території Європи.
ЕРЕ (EPE)	Платформа Європолу для експертів – провідний майданчик Європолу для експертів з правоохоронних органів, де вони обмінюються знаннями, передовими практиками та неперсоналізованими даними про злочинність.
ЄВРОПОЛ (EUROPOL)	Агентство Європейського Союзу з питань співробітництва в правоохоронних органах – правоохоронний орган Європейського Союзу, який допомагає державам-членам у боротьбі з серйозними міжнародними злочинами та тероризмом.
ФАТФ (FATF)	Міжнародна група з протидії відмиванню брудних грошей (ФАТФ) – міжурядовий орган, що встановлює стандарти, заснований для розробки політики боротьби з відмиванням грошей та фінансуванням тероризму.

ФІнСЕН FinCEN	Мережа боротьби з фінансовими злочинами – бюро Міністерства фінансів США, яке збирає та аналізує інформацію про фінансові операції.
ПФР (FIU)	Підрозділ фінансової розвідки – державний орган, відповідальний за збір, аналіз та розповсюдження фінансової інформації та розвідувальних даних про підозру у відмиванні грошей та фінансуванні тероризму.
ІП (IP)	Інтернет-протокол – зведення правил, що регулюють формат даних, які надсилаються через Інтернет або інші мережі.
ЗПО (LER)	Запит від правоохоронних органів – запит, зроблений правоохоронними органами компаніям або фізичним особам з проханням надати інформацію для проведення розслідувань.
MiKA (MiCA)	Регламент (ЄС) 2023/1114 Європейського парламенту та Ради від 31 травня 2023 року про ринки криптоактивів, а також про внесення змін до Регламентів (ЄС) No 1093/2010 та (ЄС) No 1095/2010 та Директив 2013/36/ЄС та (ЄС) 2019/1937. Це новий регламент ЄС, що регулює криптоактиви. Він набуде чинності з 30 грудня 2024 року.
ВГ (ML)	Відмивання грошей – незаконний процес отримання великих сум грошей, отриманих від злочинної діяльності, що замаскований під походження коштів із законних джерел.
Мультипідписний (криптовалютний) гаманець / мульти-сиг-гаманець (MultiSig Wallet)	Мультипідписний криптовалютний гаманець із (мультисіг-гаманець)– тип криптовалютного гаманця, який вимагає кількох приватних ключів для авторизації трансакції.
ОКЕПД (OCEEA)	Офіс Координатора економічної та природоохоронної діяльності ОБСЄ
ОБСЄ (OSCE)	Організація з безпеки та співробітництва в Європі – регіональна організація безпеки в Європі, зосереджена на сприянні діалогу та всеохоплюючому співробітництві у військовому, політичному, екологічному та економічному вимірах.
ДВД (OSINT)	Дані з відкритих джерел – інформація, зібрана із загальнодоступних джерел, яка використовується в контексті розслідування.
ПБТ (OTC)	Позабіржова торгівля – торгівля віртуальними активами між двома сторонами з використанням центральної біржі або брокера або без них.
УНЗ ООН (UNODC)	Управління ООН з наркотиків та злочинності – відомство, що діє в рамках Організації Об'єднаних Націй і відповідає за підготовку та розповсюдження даних про наркотики та злочинність.
ВАСП (VASP)	Постачальник послуг віртуальних активів – термін, введений ФАТФ для позначення суб'єкта господарювання, який проводить діяльність або операції з віртуальними активами. (Див. стор. 20 для отримання додаткової інформації).
ВПН (VPN)	Віртуальна приватна мережа – технологія, яка дозволяє створити безпечне з'єднання через менш захищену мережу між комп'ютером особи та Інтернетом, іноді, але не завжди, щоб приховати місцезнаходження користувача.

Вступ

Мета даного посібника

Цей документ є всеосяжним посібником для співробітників правоохоронних органів, включаючи поліцейських, прокурорів, державних і федеральних агентів, а також податківців і криміналістів, які нещодавно познайомилися з криптовалютами та іншими віртуальними активами. Він призначений для тих, кому все частіше доручають розслідувати злочини, пов'язані з криптоактивами.

Основна увага в ньому приділяється найпоширенішим видам шахрайства та шахрайської поведінки, пояснюються передові практики для поліцейських, які дії слід вжити та які види інформації можна отримати від потенційних жертв, особливо під час початкового збору доказів у місцевих відділках поліції.

Цей посібник був написаний і розроблений для використання правоохоронцями. Автори посібника навмисно не торкалися тих питань щодо криптовалют, які навряд чи будуть важливими у рослідуваннях поліції щодо справ за участі окремих потерпілих.

Він також спеціально акцентує увагу на взаємодії між правоохоронними органами та фізичними особами. Звіти про підозрілі трансакції STR (Suspicious Transaction Reports) або діяльність SAR (Suspicious Activity Reports), які використовуються фінансовими установами або підрозділами фінансової розвідки (або їх еквівалентами), не враховувалися.

У нинішньому способі розслідування справ про криптовалюту було виявлено кілька проблем, наприклад, через неповний збір даних слідчі повідомили, що їм довелося зв'язуватися із жертвами, щоб зібрати інформацію на кшталт адреси криптовалютного гаманця, без якої подальше розслідування неможливе. Співробітникам потрібно розуміти, яку інформацію важливо збирати, а яку – ні. Таке нерозуміння часто призводить до кількаденних затримок, оскільки жертви можуть не до кінця розуміти, яка інформація є актуальною для правоохоронних органів.

Ця прогалина в знаннях – не просто незручність; нею користуються злочинці, які з самого першого дня розуміють, що ця технологія є доступною в усьому світі, в той час як передові практики в розслідуваннях криптовалют продовжують відставати. У відповідь на цю зростаючу проблему ми розробили цей посібник, у якому описано, яким чином правоохоронні органи повинні діяти під час розслідувань і як допомагати потенційним жертвам, які повідомляють про злочини, пов'язані з криптовалютою.

Визнаючи складність теми та різноманітність правових ситуацій і практик у різних державах-учасницях ОБСЄ, наша мета полягає не в тому, щоб запропонувати вичерпний посібник, а скоріше практичний посібник, який може використовуватися на ситуативній основі правоохоронними органами першої лінії, які отримують повідомлення від громадян. Він має на меті спонукати до обговорення того, як удосконалити найкращі внутрішні практики, особливо якщо існуючі інструкції не покривають питань криптовалюти. Найбільш поширені випадки шахрайства були узагальнені в тому вигляді, в якому вони існують сьогодні, а також

надано базову інформацію для більш глибокого розуміння предмета.

Цей посібник є важливою сходинкою на шляху подолання розриву між правоохоронними органами та постійно мінливим світом віртуальних активів. Слід визнати, що простір Web3, в якому працюють криптовалюти, стрімко розвивається, і цей посібник може потребувати доповнення додатковими знаннями.

Цей посібник розповідає не лише про інструменти та стратегії, необхідні для ефективних розслідувань, але й має на меті сприяти співпраці та безперервному навчанню в громаді. Кінцева мета полягає в тому, щоб надати правоохоронцям знання та впевненість, необхідні для того, щоб протистояти унікальним викликам, пов'язаним із криптовалютними злочинами.

Структура даного посібника

Основною метою цього посібника є освіта правоохоронців, які є новачками у сфері злочинів щодо віртуальних активів, а також підтримка жертв, які повідомляють про такі злочини. З цією метою посібник має наступну структуру:

По-перше, пропонується стислий огляд цифрових активів. Цифрові активи можна розглядати як великий загальний термін, який включає криптовалюти, такі як Bitcoin і Etherium. Буде надано пояснення того, що це таке і чим вони схожі або відрізняються один від одного. Їх відмінності та подібні риси буде розглянуто для забезпечення чіткого розуміння. Крім того, будуть обговорені потенційні способи використання та зловживання криптовалютами, а також технології, які їх підтримують.

Після забезпечення базового розуміння віртуальних активів, у посібнику представлені поширені типи злочинів, пов'язаних з ними. Далі в ньому описані стандартні протоколи боротьби з цими злочинами, які з них можна швидко вирішити, а які вимагають більш ретельного розслідування. Посібник також охоплює збір доказів по кожному злочину, питання, які потрібно поставити жертві, дані, якими можна поділитися з постачальниками послуг віртуальних активів, та інформація, яку можна отримати з бірж віртуальних активів.

Доступність та спрощення термінології: Через складність галузі, автори використовували спрощену, нетехнічну термінологію, щоб зробити цей звіт доступним для початківців. Уникаючи технічних термінів, автори мали на меті запропонувати чіткий і зрозумілий контент для всіх читачів. Зрештою, посібник пропонує ресурси підтримки для жертв і представляє різні пропозиції, які можуть допомогти запобігти злочинам, пов'язаним з криптовалютою.

Довідкова інформація

Розслідування, що стосуються криптоактивів, спочатку можуть здатися важкими, особливо з огляду на хибні уявлення про складність повернення таких активів. Існує міф, що якщо національна валюта була конвертована в криптовалюту, таку як Bitcoin, кошти безповоротно втрачаються, залишаючи жертв безпорадними та змушуючи слідчих закривати справи. Таке сприйняття було вірним ще кілька років тому, але часи змінилися.

Прогрес у технологіях відкрив нові можливості, подібно до того, як перевірка ДНК дозволила знову відкрити та розкрити старі справи. Тепер ми можемо знову відкрити раніше закриті криптвалютні справи. Постійно зростаюча доступність інструментів, призначених для виявлення та перевірки криптовалютних трансакцій на блокчейні, та зміни в міжнародному праві дозволяють нам виявляти осіб, винних у кримінальних справах з використанням криптовалюти. Ці інструменти стають все більш зручними та поширеними, що віщує зміни в ландшафті розслідувань.

Незважаючи на всі ці інструменти, ми все ще бачимо, що багато розслідувань, які проводять місцеві правоохоронні органи, передчасно закриваються через обмежене розуміння та знання. Всупереч поширеній думці, трансакції з криптовалютою можна відстежити. Завдяки точному запису даних від самого початку, існує підвищена ймовірність пов'язати трансакції з потенційним підозрюваним, об'єднуючи віртуальні та матеріальні докази.

Останніми роками кілька держав-учасниць ОБСЄ почали інтегрувати криптовалюти та інші віртуальні активи у свої національні нормативні акти щодо боротьби з відмиванням грошей згідно із оновленими стандартами, виданими Групою з розробки фінансових заходів боротьби з відмиванням грошей (ФАТФ). Цей розвиток подій означає, що компанії, які працюють з криптовалютами, тепер повинні дотримуватися процесів, які були раніше розроблені для традиційних банківських установ. Їх просять перевіряти особи своїх клієнтів, ретельно вивчати джерела коштів і відстежувати, куди надсилаються криптовалюти.

Усвідомлюючи ці зміни, команда експертів ОБСЄ з віртуальних активів вирішила запустити допоміжний посібник, спеціально розроблений для представників місцевих правоохоронних органів. Цей посібник не тільки висвітлить нові можливості в розслідуваннях щодо криптовалют, але й надасть правоохоронцям знання та інструменти, необхідні для того, аби добиватися справедливості в цій складній сфері, що розвивається.


30th OSCE MINISTERIAL COUNCIL
osce NORTH MACEDONIA 2023
IT'S ABOUT PEOPLE
30 NOVEMBER 1 DECEMBER 2023
SKOPJE
Interpretation Languages
CH 0 - Floor
CH 1 - ENG
CH 2 - FRA
CH 3 - GER
CH 4 - SPA
CH 5 - RUS
CH 6 - ITA
CH 7 - ALB
CH 8 - MKD


osce
Valiant Richey
OSCE Special Representative and Co-ordinator for Combating Trafficking in Human Beings
Helga Maria Schmid
OSCE Secretary General
osce


Mariia Sulialina
Deputy Head of the Center of Civil Education "Almenda", Ukraine
Hadja Lahbib
Minister of Foreign Affairs of Belgium
Stefano Baldi
Permanent Representative of Italy to the OSCE
Dorota Woroniecka-Krzyżanowska
Polish Center for International

Про ОБСЄ

ОБСЄ є Організацією з безпеки і співробітництва в Європі. Ця регіональна організація безпеки діє з метою сприяння діалогу та співпраці, і має всеосяжний погляд на безпеку, охоплюючи все, від військово-політичного до екологічного та економічного вимірів.

ОБСЄ була створена під час холодної війни в 1975 році і наразі складається з 57 держав-учасниць. Ці держави знаходяться переважно в Європі, де зосереджена значна частина роботи ОБСЄ, але серед них й Канада і США в Північній Америці, а також такі країни, як Казахстан, Киргизстан і Узбекистан в Центральній Азії. ОБСЄ діє на принципах всеосяжної безпеки, яка охоплює військовий, політичний, економічний, екологічний і людський виміри.

У Європі ОБСЄ працює над зміцненням стабільності та розв'язанням проблем безпеки. Її основна мета полягає в тому, щоб запобігати конфліктам та сприяти регіональному співробітництву за допомогою таких механізмів, як дипломатичні переговори, ініціативи з врегулювання конфліктів та угоди про контроль над озброєннями. Крім того, ОБСЄ проводить роботу на підтримку демократії та прав людини, наприклад, моніторинг виборів.

Коли йдеться про фінансові злочини та криптозлочини, ОБСЄ допомагає боротися з цими викликами, сприяючи обміну оперативними даними та розбудові потенціалу між своїми державами-учасницями, що працює над покращенням потоку транскордонної інформації. Це важлива робота, оскільки криптозлочини за своєю природою не обмежуються однією країною або валютою, а значить і транскордонна співпраця є життєво важливою.

ОБСЄ також заохочує створення правових рамок та надійних регуляторних заходів для боротьби як з класичним відмиванням грошей, так і з фінансуванням тероризму, а також, здійснення заходів щодо виявлення та запобігання незаконній діяльності із використанням криптовалюти. Це включає забезпечення дотримання державами-учасницями міжнародних стандартів протидії відмиванню грошей (ПВГ) та фінансуванню тероризму (ПФТ).

На допомогу цій діяльності ОБСЄ проводить навчальні програми та семінари з метою покращення експертизи правоохоронних органів, фінансових установ та інших відповідних суб'єктів у боротьбі з фінансовими та криптовалютними злочинами. Ці зусилля спрямовані на вдосконалення методів розслідування та використання передових технологій для виявлення та боротьби з кіберзлочинністю та злочинною діяльністю, пов'язаною з криптовалютами.

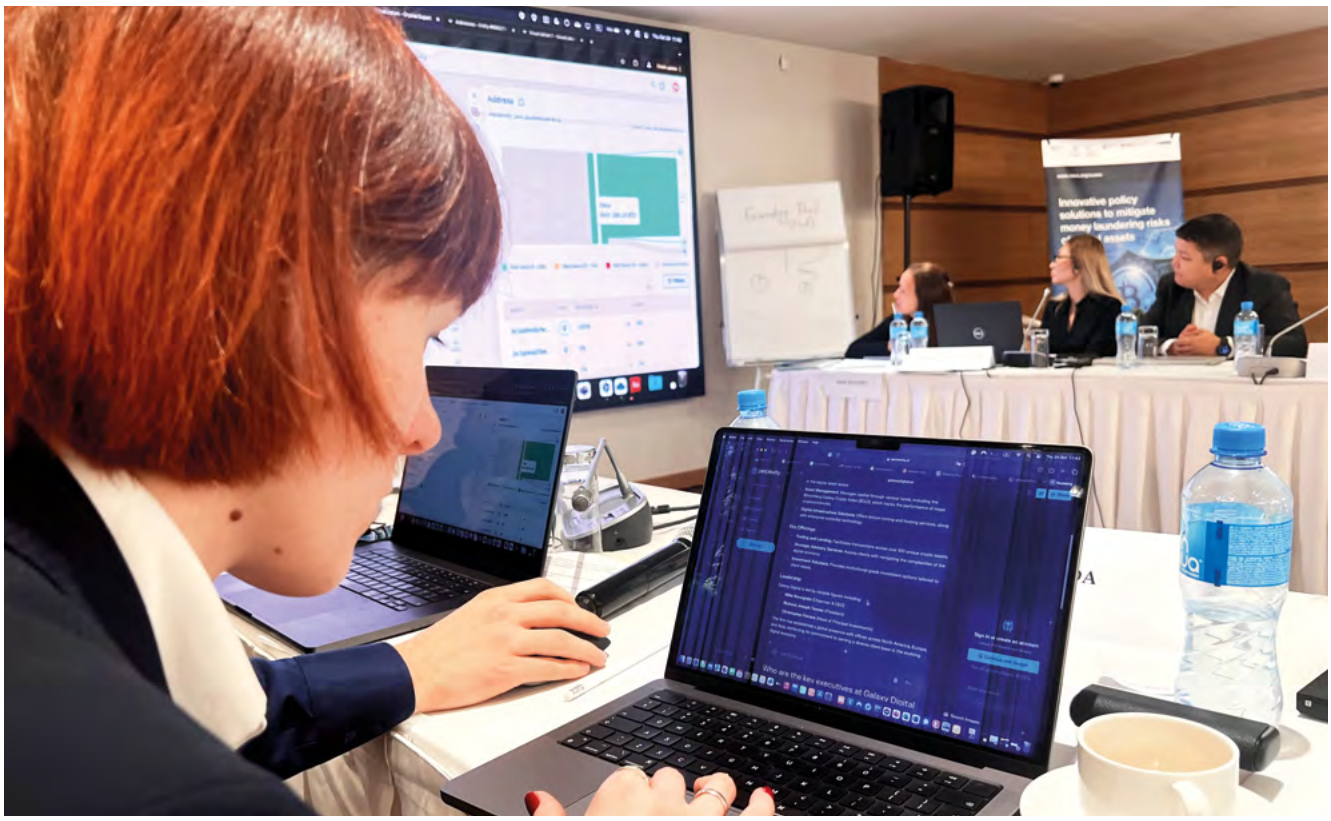
Цією публікацією ОБСЄ відповідає на потребу конкретних держав-учасниць у реагуванні на ризики, пов'язані із використанням віртуальних активів у кримінальних цілях та для обходу міжнародних санкцій. Таке подолання ризиків є основною метою проекту «Інноваційні політичні рішення для зниження ризиків відмивання грошей, пов'язаних з віртуальними активами», який очолює Офіс Координатора ОБСЄ з економічної та природоохоронної діяльності (OCEEA).

Кінцевою метою цього проекту є розбудова спроможностей національних органів влади для протидії особливим вразливостям, пов'язаним з цими віртуальними активами. Протягом усієї реалізації проекту OCEEA разом із Глобальною програмою боротьби з відмиванням грошей Управління ООН з наркотиків та злочинності (UNODC GPML) продовжувала надавати допомогу трьом країнам у Східній Європі та на Кавказі — Грузії, Молдові та Україні — у приведенні нормативно-правової бази своїх віртуальних активів (ВА) та постачальників послуг віртуальних активів (VASP) у відповідність до Рекомендацій ФАТФ з одночасним наданням відповідним правоохоронним органам цих трьох країн допомоги у розбудові потенціалу та технічної підтримки.

Для підвищення ефективності проекту команда ОБСЄ співпрацює з УНЗ ООН, яке надало свою внутрішню експертизу та практичні навчальні програми з питань криптовалют, ризиків відмивання грошей (ВГ) та фінансування тероризму (ФТ), розслідування, арешту та конфіскації, регулювання та належної перевірки клієнтів. OCEEA продовжує надавати підтримку відповідним органам, таким як центральні банки, відділи комплаєнсу ключових фінансових установ, підрозділи фінансової розвідки, генеральні прокуратури, міністерства юстиції та внутрішніх справ, допомагаючи в розробці нормативних актів та інструкцій для персоналу, організовуючи заходи з підвищення обізнаності та сприяючи міжвідомчому та міжнародному співробітництву в розслідуванні криптовалютних злочинів.

Ця публікація була створена в рамках інноваційних політичних рішень щодо зниження ризиків відмивання грошей у проектах віртуальних активів, що фінансуються Німеччиною, Польщею, Румунією, Великою Британією та Сполученими Штатами.

ОБСЄ Організація з безпеки та співробітництва в Європі



Грета Баркаускієне проводить семінар для слідчих в Астані, Казахстан. Спираючись на свій великий досвід експерта з питань протидії відмиванню грошей та координатора національної групи тактичного співробітництва Литовського центру передового досвіду з протидії відмиванню грошей, вона використовує найкращі практики як державних, так і приватних зацікавлених сторін для розширення можливостей країн-бенефіціарів.

Семінари розслідувачів, що відбулися в Тбілісі, Грузія, були зосереджені на ключових аспектах конфіскації криптовалютних активів, включаючи підготовку безпечних умов для потенційної конфіскації. Ці семінари були тісно пов'язані з подальшими вправами, спрямованими на вдосконалення навичок виявлення, передачі та відновлення криптовалютних активів на блокчейні. Фото: Міхал Громек.

Розуміння цифрових активів – посібник простою мовою

Розуміння цифрових активів – посібник простою мовою

У цьому розділі ми розглянемо відмінності між різними цифровими активами, фіатними грошима і криптовалютами. Ми також розглянемо відмінності між різними типами криптовалют та інфраструктурою побудованою навколо них.

Часто виникає плутанина щодо того, в чому полягає різниця між цифровими активами, віртуальними активами, криптоактивами та криптовалютою.

Простіше кажучи, **цифровий актив** – це дуже широкий термін. Це актив, який існує в цифровій формі. Сюди входять зображення, відео, музика, як, наприклад, файли у форматі MP3, документи та віртуальні валюти.

Віртуальний актив – це вужчий набір цифрових активів. Згідно з ФАТФ,[1] віртуальні активи (криптоактиви) – це будь-яке цифрове представлення вартості, яким можна торгувати в цифровому вигляді, передавати або використовувати для оплати. Цей термін не включає цифрове представлення фіатних валют.

На противагу цьому, **криптоактив займає** ще вужчу нішу. Це актив, який зберігає вартість, але має бути переданий за технологією розподіленого реєстру (DLT). Блокчейн – це різновид DLT. Ви можете мати віртуальний актив, як-от монету (coin), в онлайн-грі, який не є криптоактивом, оскільки він передається між гравцями в грі без використання технології розподіленого реєстру.Блокчейн на даний момент є найбільш відомим типом технології розподіленого реєстру, але існують інші технології DLT, такі як Hashgraph, Iota Tangle, R3 Corda та багато інших. Для цілей цього посібника ми зосереджуємося на фінансах на основі блокчейну.

Існує багато різних типів цифрових активів, включаючи криптовалюти, які є новими типами валюти, що працюють за технологією блокчейн, і невзаємозамінні токени (NFT), які є активами на основі зображень.

Таким чином, якщо криптоактив було створено для торгівлі, передачі або використання для оплати, ми будемо називати його криптовалютою. Ви також можете зіткнутися з терміном віртуальна валюта, який часто використовується як синонім криптовалюти. Відмінністю між криптовалютою та віртуальною валютою є технологія, що лежить в її основі.Криптовалюти використовують блокчейн, тоді як віртуальні валюти не обов'язково побудовані на блокчейні.

Цей посібник переважно буде зосереджений на злочинах, скоєних з використанням криптовалюти.

З дозволу автора (Олександра Андхов, Обчислювальне право, Карнов, 2022)

1 Група з розробки фінансових заходів боротьби з відмиванням грошей, джерело: https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies (станом на 26 вересня 2023 року)

Порівняння криптовалют і фіатних валют

Традиційні монети та паперові гроші, відомі як «фіатна валюта», були основою наших економік протягом століть. Але з розвитком технологій з'явилися нові форми грошей, які розмивають межі між матеріальним і віртуальним. Коли фізичні особи здійснюють електронні перекази фіатної валюти від однієї особи до іншої – вони використовують «електронні гроші». Електронні гроші, або е-гроші, представляють звичну нам фіатну валюту в цифровій формі, що забезпечує здійснення електронних трансакцій без зміни їх вартості. Електронні гроші – це цифрове представлення фіатної валюти.

На відміну від фіату, криптовалюти працюють у децентралізованому середовищі. Вони не пов'язані з жодним урядом чи центральним банком, і різні фактори, включаючи попит, технології та довіру, визначають їхню вартість. Bitcoin, провідне ім'я в цій сфері, продемонстрував потенціал цих валют, вартість яких злетіла до неабияких висот. Ще у 2021 році вона досягла понад 64 000 доларів за монету. Криптовалюти, такі як Bitcoin і Tether, не гарантуються жодним урядом або центральним банком. Незважаючи на те, що віртуальні валюти не такі старі, як фіатна валюта, вони не такі нові, як більшість людей припускає. Одна з перших віртуальних валют — E-Gold — була представлена вже майже 30 років тому, у 1996 році.

Огляд E-Gold

Одна з перших популярних віртуальних валют називалася «E-Gold». Вперше створена в 1996 році Дугласом Джексоном і Баррі Дауні, компанія E-Gold дозволила користувачам відкривати рахунки з вартістю, вираженою в грамах золота (або інших дорогоцінних металів), і здійснювати миттєві перекази вартості на інші рахунки E-Gold.

У 2005 році E-Gold мала 2,5 мільйона власників рахунків, які виконували щоденні транзакції на загальну суму 6,3 мільйона доларів США. Він був популярним завдяки своїй ефективності, низьким комісіям та глобальній доступності. Однак, відсутність жорстких правил також приваблювала незаконну діяльність. У 2007 році компанію E-Gold було визнано винною судом присяжних у Сполучених Штатах, за обвинуваченням у відмиванні грошей, змові та веденні неліцензованого бізнесу з переказу грошей, що в кінцевому підсумку призвело до закриття E-Gold судами США в 2009 році. E-Gold породив цілий ряд наслідувачів, таких як e-Bullion.com, Pecunix.com та інші.[2]

При обговоренні цієї сфери важливо бути конкретним, оскільки термін віртуальна валюта може відноситися як до електронних грошей, так і до криптовалют. Це може швидко створити плутанину. У цьому посібнику ми зосередимося на криптовалютах.

Базова технологія: блокчейн (Blockchain)

Блокчейн – це тип технології розподіленого реєстру (DLT). Уперше ця нова технологія з'явилася 2008 року – її було описано в науково-технічній статті, опублікованій Сатоші Накомото.[3] Вона вважається децентралізованою, оскільки не має єдиного центру управління або відповідальної особи.Натомість, зміни може внести будь-який користувач, але вони повинні бути прийняті більшістю користувачів аби стати постійними.

Існує багато різних блокчейнів. Блокчейн просто відноситься до базової технології. Уявіть собі кожен блокчейн як будівлю. Вони можуть виглядати дуже по-різному зовні, і кожна будівля може мати дуже різне призначення, але якщо заглянути всередину, майже всі будівлі були побудовані з цегли та цементу.

Як і у випадку з будівлями, до деяких блокчейнів може отримати доступ будь-хто без дозволу, тоді як деякі

2 «Федеральні органи звинувачують E-Gold у допомозі кібершахраям», NBC News, травень 2007 р. (Доступно: http://redtape.nbcnews.com/_news/2007/05/02/6346006-feds-accuse-e-gold-of-helpingcybercrooks (Дата звернення: 24 серпня 2023 року). «Валютна фірма в Інтернеті визнає себе винною у відмиванні грошей», The Industry Standard, липень 2008 р. Доступно за адресою: http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering (дата звернення: 24 серпня 2023 р.). *Короткий зміст книги «Транзакції з електронним золотом»* (1996) E-Gold. Доступно за адресою: http://www.e-gold.com/unsecure/synopsis.htm (дата звернення: 24 серпня 2023 р.).

3 Накамото, С. (2008) Одноранговa електронна грошова система, Bitcoin. Доступно за адресою: https://bitcoin.org/en/bitcoin-paper (дата звернення: 26 серпня 2023 р.).

вимагають схвалення, перш ніж вам буде дозволено приєднатися.

У зв'язку з цим ми розрізняємо публічні та приватні блокчейни. Публічні блокчейни називаються «такими, що не потребують дозволу» і, як правило, вимагають меншої прозорості або контролю, тоді як блокчейни «що потребують дозволу» часто використовуються для корпоративних цілей і вимагають схвалення особи, яка бажає приєднатися.

Блокчейн називається так тому, що користувачі додають або змінюють «блоки» даних, і ці блоки пов'язані між собою в ланцюжок у хронологічному порядку (за часом). Коли один користувач робить або завантажує новий блок (наприклад, нову трансакцію з Bitcoin), всі інші користувачі блокчейну повинні перевірити новий блок за допомогою «методів консенсусу» (це включає в себе досить складні математичні рівняння), щоб переконатися, що йому можна довіряти. Оскільки всі блоки пов'язані між собою, майже неможливо перейти до попереднього блоку та змінити його. Це означає, що система не може бути підроблена. Будь-яка нова інформація, в тому числі зміна старої інформації, записується в новий блок.

Блокчейн працює, дозволяючи всім користувачам, підключеним до цього ланцюга, бачити всю історію ланцюга («бухгалтерська книга»). Таким чином, за допомогою блокчейну користувачі Bitcoin можуть бачити кожну трансакцію, що відбулася. Це дозволяє слідчим проводити розслідування. Через розподіл реєстру блокчейну до кожного користувача, блокчейн називається «технологія розподіленого реєстру» або DLT. Це як «таблиця Google», над якою кожен може співпрацювати та бачити попередні версії. Оскільки все видно і не може бути змінено без того, щоб всі могли це бачити, існує високий рівень прозорості, довіри та безпеки. Існує також високий рівень стійкості до атак — оскільки кожна людина має копію блокчейну, а централізованої версії не існує, навіть якщо один користувач («вузол» у термінології блокчейну) зазнає атаки та зазнає ураження, система все одно може працювати.

З дозволу автора (Олександра Андхов, Обчислювальне право, Карнов, 2022).

Види криптовалют

Існує два способи розрізнення криптовалют:

- **Чи є вони конвертованими чи неконвертованими**
- **Чи є вони централізованими чи децентралізованими**

Ці відмінні характеристики описані нижче.

Конвертовані танеконвертовані валюти

Конвертовані валюти мають еквівалентну вартість у фіатній валюті і можуть бути обміняні зворотнім чином на «звичайні» гроші. Ця конвертованість не гарантується, оскільки криптовалюти не підтримуються жодним урядом чи установою. Конвертованість криптовалюти у фіатну валюту ґрунтується на прийнятті ринкових і приватних пропозицій. Це той тип криптовалюти, з яким найчастіше трапляються злочини. Приклади конвертованих валют включають Bitcoin та E-Gold.

Неконвертовані валюти схожі на золоті монети, які залишаються в комп'ютерній грі. Злочини, скоєні з їх допомогою, менш ймовірні, оскільки вони не мають реальної ринкової вартості. Менш із тим, деякі люди знаходять спосіб обміняти їх поза межами гри, в якій вони існують, що робить їх конвертованими поза грою, навіть якщо це суперечить правилам гри. Наприклад, хтось може передати «зібрані золоті монети» від одного гравця іншому гравцеві в грі, при

цьому трансакція олачується в офлайні готівкою.

Централізовані та децентралізовані валюти

Централізовані криптовалюти контролюються єдиним органом, який випускає валюту, встановлює її правила, веде книгу платежів і має право вилучати її з обігу.

Централізовані валюти можуть бути конвертованими або неконвертованими. Неконвертовані валюти завжди централізовані (оскільки, наприклад, не можна мати валюту в грі без того, щоб гра адмініструвала валюту). При обміні централізованої конвертованої валюти курс валют визначається ринковим попитом і пропозицією, або він фіксується адміністратором. Хорошим прикладом централізованої валюти є E-Gold.

З іншого боку, децентралізовані валюти не мають центрального органу та працюють на основі одноранговой мережі. Уявіть децентралізовану систему, таку як Інтернет. Так само, як немає одного керівника, відповідального за весь Інтернет, децентралізована система не має одного головного контролера. Незважаючи на те, що більшість людей щодня користуються Інтернетом, немає єдиної компанії, яка б отримувала оплату; натомість, різні провайдери стягують оплату за різні послуги. Таким самим чином використовується технологія мережі блокчейн, що лежить в основі криптовалют, таких як Bitcoin.Управління трансакціями здійснюється через мережу, і жоден інший моніторинг з боку будь-якого органу влади не здійснюється.

Нижче наведено добірку з десяти криптовалют із найбільшою ринковою капіталізацією станом на 23 серпня 2023 року, згідно з посиланням у виносці.[4]

Назва	Символ	Ринкова капіталізація (станом на 24 серпня 2023 р.)	Порівняння з валовим внутрішнім продуктом наступних країн[5]
Bitcoin	BTC	$514,912,135,787	Судан
Ethereum	ETH	$201,475,414,760	Гаїті
Tether USDt	USDT	$82,835,552,223	Сомалі
BNB	BNB	$33,285,580,473	Андорра
XRP	XRP	$27,991,699,189	Кюрасао
USD Coin	USDC	$26,005,195,827	Лесото
Cardano	ADA	$9,357,776,591	Сент-Вінсент і Гренадини
Dogecoin	DOGE	$8,965,846,112	Північні Маріанські острови
Solana	SOL	$8,792,761,272	Самоа
TRON	TRX	$6,938,358,042	Американське Самоа

Псевдовалюти та анонімні токени

Псевдо-анонімні валюти передбачають облікові записи, які використовують псевдоніми, що означає, що хоча трансакції не пов'язані безпосередньо з особами, деяка ідентифікаційна інформація залишається. Наприклад, типовий банківський рахунок у фіатній валюті, який використовується для покупки криптовалюти, пов'язаний з даними, які можна ідентифікувати. Монети в цій категорії включають Bitcoin та Ether.

Натомість, анонімні токени забезпечують більшу анонімність, використовуючи передові криптографічні методи для приховування деталей трансакції та пов'язаних з нею осіб, що ускладнює їх відстеження до початкового користувача. Прикладами таких токенів є Monero та Zcash.

4 Усі криптовалюти (2023) CoinMarketCap. Доступно за адресою: https://coinmarketcap.com/all/views/all/ (дата звернення: 24 серпня 2023 р.).
5 На основі даних Світового банку про ВВП (за поточним курсом дол. США), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false (станом на 23 серпня 2023 року).

Криптогаманці

Криптовалютний гаманець – це місце, де зберігається криптовалюта. Можна провести аналогію уявивши як сьогодні зберігаються гроші по всьому світу.

Гроші існують у різних формах. Частина з них зберігається в золотих злитках, розміщених у великих банках, частина циркулює у вигляді паперових банкнот, банківських переказів онлайн або криптовалют. Криптовалютні гаманці мають різні форми – додаток на телефоні, пристрій, схожий на USB-накопичувач, або просто програмне забезпечення (трохи схоже на вашу адресу електронної пошти), до якого у вас буде доступ після введення логіна та пароля. Незважаючи на те, що існують різні види криптовалютних гаманців, вони використовують одну і ту ж технологію. Більшість з них мають паролі для відновлення з 12, 18 або 24 слів, які можуть повторно відкрити гаманець.

Адреси криптогаманців

Адреси криптовалютних гаманців схожі на номери банківських рахунків. Мати номер чийогось банківського рахунку не означає мати доступ до чиїхось грошей. Адреси криптогаманців мають довгі, складні послідовності з безліччю чутливих до регістру літер і цифр. Ось два приклади:

Криптовалютний гаманець для валюти TRON
TYm3NTSyk85t9UHSd68DY4vGWQADHXpaXJ

Криптовалютний гаманець для Bitcoin
Bc1qu5z7kn0v2krhglsnan4c0m5f76xk69p53wjwgh

Різниця між традиційними номерами банківських рахунків та адресами криптогаманців полягає в тому, що в порівнянні з адресою криптогаманця з номера банківського рахунку можна отримати більше інформації.

Правоохоронні органи можуть легко розшифрувати номер IBAN та звернутися до відповідного органу.

IBAN – це міжнародний номер банківського рахунку. У ньому може бути до 34 букв і цифр.

Він складається з коду країни, двозначного коду безпеки, а потім реквізитів про банк і рахунок. Іноді в різних країнах ці банківські реквізити форматуються по-різному. Наприклад:

IBAN:

- **LT44 32500 47338696265**

  LT означає Литовську Республіку,

  32500 означає «Револют Банк» Revolut Bank UAB

  47338696265 – це номер облікового запису користувача[6]

Якщо такий номер банківського рахунку IBAN з'явиться в розслідуванні, співробітник знатиме, що потрібно звернутися до литовського банку Revolut. Ця інформація можебути отримана від так званих «валідаторів IBAN», таких як iban.com або https://wise.com/gb/iban/checker. Після цього можна приступати до процесу отримання особистої інформації про власника рахунку.

У випадку псевдоанонімних криптовалют на кшталт Bitcoin, жоден правоохоронний орган не зможе отримати особисту інформацію про власника рахунку на основі такого номера рахунку: bc 1qu5z7kn0v2krhglsnan4c0m5f76xk-69p53wjwgh.

Для того, щоб знайти ідентифікаційну інформацію власника, необхідне спеціалізоване програмне забезпечення, як, наприклад, **постачальник блокчейн аналітики**.

Постачальники блокчейн аналітики можуть розкривати ідентифікаційну інформацію користувачів і відстежувати трансакції між різними криптовалютами, що є поширеною тактикою яка використовується щодо викрадених криптовалют. Здатність таких провайдерів

6 IBAN та коди фінансових установ, Банк Литви, https://www.lb.lt/en/iban-and-financial-institution-codes (станом на 25 вересня 2023 року).

ідентифікувати, які фінансові установи або криптобіржі (VASP – надавачі послуг віртуальних активів) мають цю ідентифікаційну інформацію, залежить від законодавства країни, в якій вони працюють. З цієї причини міжнародні організації, такі як ОБСЄ, допомагають державам-учасницям запровадити кращі міжнародні практики в цій сфері.

Оглядачі криптогаманців

Оскільки провідні типи публічного блокчейну відкриті для всіх, можна переглянути всі трансакції, які відбуваються в гаманці, за допомогою «оглядача криптогаманця».

Оглядач криптогаманця – це пошукова система, розроблена спеціально для навігації даними блокчейну. Він надає детальну інформацію про окремі блоки, трансакції та пов'язані з ними гаманці. Сприймайте це як "Google" для трансакцій на блокчейні.

Увага:

Для кожного типу криптовалюти може знадобитися окремий провідник гаманця. Для цього слід ввести назву криптовалюти, яку ви хочете переглянути, і додати вираз «оглядач гаманця» або «оглядач блокчейну» в пошукову систему для огляду провідних провайдерів. Такі послуги, як правило, безкоштовні.

Основні способи використання провідників криптогаманців:

- **Перевірка трансакцій:** Оглядачі гаманців дозволяють користувачам підтвердити, що трансакція відбулася. Коли хтось стверджує, що відправив криптовалюту, для підтвердження цього можна використовувати провідник, шукаючи трансакцію за допомогою ідентифікатора трансакції або адреси гаманця.
- **Аудит та ведення записів:** Для фізичних осіб або компаній, яким потрібно вести записи про трансакції, оглядачі можуть надати детальну інформацію про те, коли відбулася трансакція, яку суму було відправлено, та задіяні адреси.
- **Дослідження та аналіз:** Розробники, дослідники та аналітики часто використовують оглядачі гаманців для вивчення загального стану та активності блокчейну. Вони можуть бачити, скільки трансакцій відбувається, розмір трансакцій тощо.
- **Баланс гаманця:** Вводячи адресу гаманця в оглядач, можна переглянути баланс конкретного криптовалютного гаманця та переглянути історію його трансакцій.

Безкоштовні оглядачі гаманців: Легко знайти оглядачі криптогаманців для кожного типу криптовалюти, просто ввівши «найкращий безкоштовний провідник криптовалютного гаманця XXX» у звичайну пошукову систему в Інтернеті.

Використовуючи ці інструменти, будь-хто може досліджувати та перевіряти трансакції в блокчейні, навіть не володіючи криптовалютою або не маючи глибоких знань про технологію. Так само, як ми можемо шукати в Інтернеті за допомогою надійних пошукових інструментів, ми можемо шукати блокчейни.

Обмін криптовалют

Подібно до «звичайних» грошей, потрібно використовувати спеціальну платформу для обміну одного типу криптовалюти на інший, або на фіатну валюту. Існує три основних типи платформ: одноранговi біржі (P2P), централізовані обмінники (CeX) та децентралізовані обмінники (Dex).

P2P розшифровується як **peer-to-peer**, а отже, person-to-person або, частіше, user-to-user (оскільки юридичні особи можуть продавати або пропонувати свої активи). Тут користувачі купують не у самої біржі, а в інших користувачів. Прикладом такої P2P-біржі, яка припинила свою діяльність, став фінський провайдер під назвою LocalBitcoin.com.

Такі обмінники продають власні віртуальні активи і не зводять користувачів один з одним.

Одноранговi обміни регулюються ПВГ й ПФТ[7] і вимагають детальної інформації про користувачів. Вони також повинні дотримуватися певних правил у країнах, де вони працюють.

Децентралізовані біржі стверджують, що вони функціонують як автоматичні конвертери файлів (наприклад, .doc в .pdf). Вони в основному використовуються для трансакцій між криптовалютами і рідше для обміну фіатної валюти у криптовалюту.. Кошти, що задіяні у децентралізованих обмінах, потребують спеціалізованої підтримки для відстеження.

Це лише верхівка айсберга. Також з'являються нові типи бірж, такі як децентралізовані біржі, позабіржові біржі, міксери та тумблери. Це технологія, що стрімко розвивається, яка розробляється з метою приховування слідів трансакцій користувачів. Багато держав-учасниць ОБСЄ вживають заходів для обмеження використання таких інструментів.

Міксери та тумблери

Міксери та тумблери – це послуги, призначені для підвищення конфіденційності та анонімності криптовалютних трансакцій. Їх основна функція полягає в змішуванні коштів різних користувачів, тим самим маскуючи джерело походження коштів.

Міксери
Це централізовані або децентралізовані сервіси, які змішують криптовалютні кошти

7 Це стосується лише криптобірж, що працюють у країнах, які імплементували рекомендацію ФАТФ 15, яка вимагає від країн включити фінансові установи, що займаються криптовалютами, у свою структуру AML та CTF.

з різних джерел, щоб приховати їх походження. Користувачі відправляють свої криптовалюти (наприклад, Bitcoin) на міксер, який потім перемішує ці монети з коштами інших користувачів або власними монетами. Як тільки «процес змішування» завершується, сервіс надсилає еквівалентну суму монет за вирахуванням комісії на вказану користувачем адресу, що ускладнює відстеження походження монет. Однак централізовані міксери керуються однією сутністю, яка потенційно може реєструвати трансакції. Група експертів EC3 Європолу пропонує курси з «розділення», доступні лише для офіційних представників правоохоронних органів.

Подібні до міксерів послуги в традиційній банківській справі

Міксери працюють аналогічно звичайним банкам, де розміщаються і знімаються кошти. Розглянемо велику фінансову установу, куди вкладають гроші різні фізичні особи. Якби ця установа агрегувала всі ці депозити, а потім розподіляла їх між власниками рахунків без зазначення походження кожного долара, це нагадувало б процес змішування. Кошти контролюються відомою сутністю, такою як централізований міксер, і потрапляючи всередину, ці кошти змішуються з іншими. Провідні постачальники аналітики блокчейну стверджують, що пропонують послуги автоматичного або ручного «розділення» для більшості провідних міксерів, що дозволяє цим постачальникам переглядати транзакції в таких сервісах.[8]

Тумблери

Тумблери схожі на міксери, і в багатьох контекстах ці термінивзаємозамінні. Основною метою тумблера також є покращення конфіденційності трансакцій. Деякі розглядають тумблери як більш досконалі варіанти міксерів. Вони використовують передові алгоритми, щоб переконатися, що змішані монети не можуть бути пов'язані з їхніми першоджерелами.

Подібні до тумблерів послуги в традиційному банкінгу

Тумблери можна порівняти з банківськими рахунками в країнах, які визначені як податкові гавані, або з офшорними банками, які славляться тим, що пропонують підвищену конфіденційність і приватність. Такі банки зазвичай використовують складні структури та послуги, адаптовані для конфіденційності та захисту активів. У сфері криптовалют тумблери використовують передові математичні алгоритми для підтримки анонімності трансакцій, забезпечуючи більш витончений рівень приховування, ніж стандартні міксери. Відстеження трансакції через тумблер є складним і трудомістким, але не неможливим.

Відмінності та порівняння

Незважаючи на те, що і міксери, і тумблери служать одній меті – підвищенню конфіденційності трансакцій, відмінності між ними часто зводяться до їх методів і рівня витонченості. Це все одно, що порівнювати базові веб-браузери з тими, які пропонують розширені функції конфіденційності. Обидва сервіси дозволяють вам переглядати веб-сторінки, але один пропонує більш просунуті інструменти для збереження анонімності.

Постачальники послуг віртуальних активів (VASP) і постачальники послуг криптоактивів CASP

Постачальник послуг віртуальних активів (VASP) здійснює такі види діяльності:

- Забезпечення обміну між віртуальними активами та фіатними валютами;
- Забезпечення обміну між однією або декількома формами віртуальних активів;
- Забезпечення переказу віртуальних активів з одного гаманця на інший,
- Надання фінансових послуг, пов'язаних з продажем віртуальних активів.

Існує ряд термінів, які використовуються як синоніми, коли мова йде про VASP. Термін «VASP» було прийнято Групою з розробки фінансових заходів боротьби з відмиванням грошей (ФАТФ). Однак термін «CASP», що означає постачальника послуг криптоактивів, зазвичай використовується в ЄС замість VASP. Кількість послуг, визначених у рамках CASP, є ширшою, ніж у VASP. Також іноді використовуються терміни «біржі» і «брокери», але вони представляють лише один з багатьох типів VASP або CASP.

8 Автор не зміг підтвердити або спростувати ці твердження до кінцевого терміну редакційної публікації.

Протокол розслідування злочинів, пов'язаних із цифровими активами

Протокол розслідування злочинів, пов'язаних із цифровими активами

Чотири найважливіші типи інформації, яку потрібно зібрати

Коли потенційна жертва приходить до поліцейської дільниці та стверджує, що стала об'єктом шахрайства з криптовалютою, необхідно зібрати чотири важливі фрагменти інформації.

Транзакції з криптовалютою є незворотними – після того, як вони будуть завершені та потраплять у блокчейн, потрібно буде докласти значних зусиль, щоб повернути ці кошти жертві. І все ж, хоча зусилля дійсно значні, це не є неможливим.

Час

Першим ключовим елементом є час. Криптовалютні трансакції не завжди відразу потрапляють у блокчейн. Часто є певний проміжок часу, коли кошти зберігаються в банку або у ліцензованого криптовалютного брокера, перш ніж бути записаними в блокчейні. Встановити, чи це так, є першим і найважливішим питанням, оскільки це дає можливість скасувати трансакцію.

Фінансова установа

Наступне за важливістю питання – запитати у потерпілого, яким криптовалютним брокером або фінансовою установою він користувався під час переказу фіатної валюти.

Якщо переказ був здійснений брокеру в юрисдикції з низьким рівнем ризику, яка забезпечила дотримання правил боротьби з відмиванням грошей у фінансових установах, є ймовірність, що трансакцію можна зупинити.

Розмір

Третім за важливістю питанням є розмір трансакції, оскільки великі суми коштів, що є більшими за поріг боротьби з відмиванням грошей, підлягають перевірці VASP або CASP. Якщо жертва здійснила великий переказ на ліцензовану біржу, можливо, вдасться звернутися до цієї біржі та зупинити її конвертацію в криптовалюту.

Тип криптовалюти

Нарешті, останнє ключове питання полягає в тому, який тип криптовалюти або віртуального активу був куплений. Деякі типи можна легко простежити, наприклад, Bitcoin. Інші типи криптовалют, відомі як конфіденційні монети, такі як Monero та ZCash, були розроблені для того, щоб зробити відстеження та розслідування складнішим, але навіть їх можна простежити, доклавши певних зусиль.

Якщо трансакція з банківського рахунку жертви відбулася зовсім нешодавно, слід докласти всіх зусиль для того, щоб зупинити її потрапляння в блокчейн. Отримання справи в дільниці та передача її для досудового розслідування іншим колегам, які можуть забрати її через кілька днів, може значно знизити шанси на успіх.

Ось три приклади, які є поширеними та ілюстративними для цієї концепції:

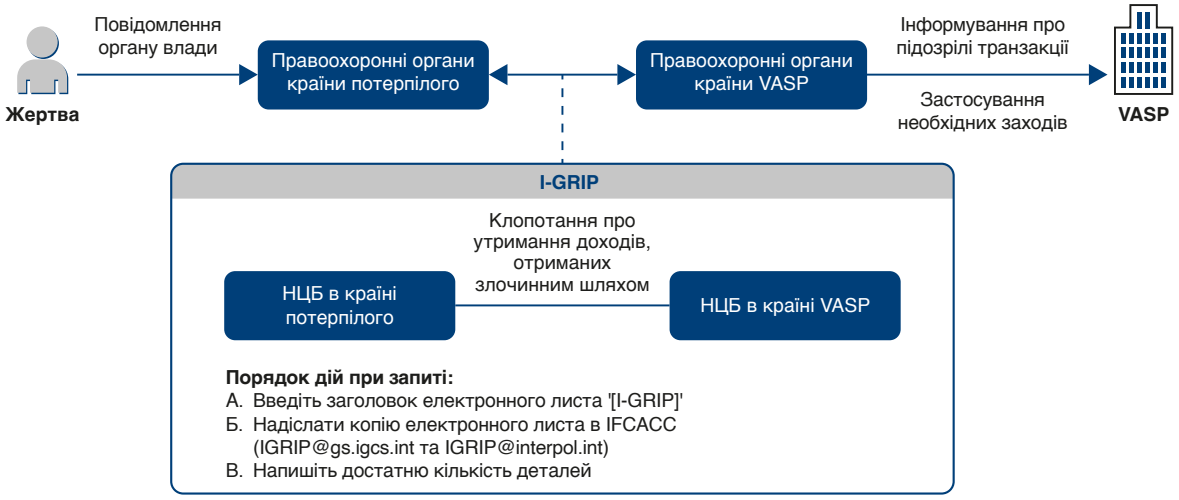
Приклад 1: Якщо у справі потенційної жертви переказ фіатної валюти з міжнародного банку ініціюється, наприклад, у п'ятницю ввечері, та про це повідомляють правоохоронцям у суботу вранці, тоді ще можна звернутися до банку та зупинити трансакцію. Якщо потерпілий не звернувся до банку, йому слід негайно це зробити. (Див. рішення Інтерполу у справі IGrip, стор. 23)

Приклад 2: Навіть якщо жертва перевела більшу суму зі свого банківського рахунку криптовалютному брокеру, а переказ уже покинув рахунок жертви, на банківському рахунку клієнта може бути інформація із назвою VASP/CASP, якому було надіслано переказ. У цьому прикладі, якщо переказ був відправлений одному з великих брокерів, таких як Binance, клієнт повинен негайно зв'язатися зі своєю службою підтримки клієнтів через вікно чату або надіслати електронний лист із заголовком: **"Терміново: Зупиніть обмін – шахрайство"** на адресу fraud@nameofthebroker.domain або compliance@nameofthebroker.domain та поінформувати їх про те, що переказ, який надходить від конкретного IBAN, певного розміру та в конкретні терміни, не підлягає обробці.

Співробітники правоохоронних органів також можуть вимагати призупинення коштів, наприклад, за допомогою системи запитів на державні правоохоронні органи Binance: https://www.binance.com/en/support/law-enforcement.
Великі брокери або біржі та інші VASP зазвичай мають певну процедуру, яка може допомогти правоохоронним органам виявити та зупинити переказ. Більшість гравців у галузі мають адреси електронної пошти, як-от compliance@name-of-the-broker.com або fraud@name-on-of-the-broker.com, які можна використовувати для повідомлення про термінові випадки.

У той же час, правоохоронний орган країни потерпілого може зробити

Робочий процес <I-GRIP>[9]



Джерело: Зображення надане Інтерполом

запит на зупинку платежу через Інтерпол за допомогою інструменту під назвою **Глобальне оперативне переривання платежів** і (I-GRIP). Це канал зв'язку з правоохоронним органом тієї юрисдикції, в якій знаходиться постачальник послуг віртуальних активів (VASP. Інтерпол запустив інструмент I-GRIP, щоб зробити міжнародне співробітництво достатньо швидким для здійснення початкових етапів повернення активів.

Як тільки правоохоронний орган юрисдикції, де знаходиться постачальник послуг віртуальних активів (VASP), отримає запит I-GRIP, він може вжити необхідних заходів для утримання доходів, отриманих злочинним шляхом, від подальшої обробки відповідно до свого національного законодавства. Необхідні заходи можуть набувати різних форм. Вони можуть просто повідомити одержувача VASP про підозрілу трансакцію, щоб VASP міг здійснити власне добровільне ділове рішення про призупинення підозрілого рахунку або навіть про відкликання трансакцій. Крім того, правоохоронні органи можуть використовувати свої адміністративні повноваження, щоб зобов'язати VASP призупинити дію підозрілого облікового запису. Крім того, правоохоронний орган може відкрити власне національне кримінальне розслідування паралельно з розслідуванням, що проводиться юрисдикцією, що здійснила запит I-GRIP, та видати постанову про арешт підозрілого рахунку за підозрою у кримінальній діяльності.

Якщо правова база в державі-учасниці ОБСЄ це дозволяє, іншою можливістю може бути негайне порушення справи разом із повідомленням потенційного потерпілого, оскільки час є одним із найважливіших аспектів у криптовалютних розслідуваннях.

Приклад 3: Якщо потенційна жертва не до кінця впевнена, якому криптовалютному брокеру були відправлені кошти, а на реквізитах переказу є абревіатури букв і цифр, які виглядають схоже на наступне:

`1C5Eu4UpeK5djG3QiKwhcLELtFwHT146dG`

це може вказувати на те, що кошти були або будуть обміняні на криптовалютний гаманець. Такі гаманці можна порівняти з банківськими рахунками або поштовою скринькою, де зберігаються кошти. При наявності певних навичок, кошти в такому гаманці можна відновити або заморозити. Навіть незважаючи на те, що таке поєднання букв і цифр виглядає незвично для осіб, які не знайомі з криптовалютою, для слідчих, які мають досвід у цій сфері, такі комбінації букв і цифр надають інформацію, схожу на номер кредитної картки. Наявність адреси криптовалютного гаманця схожа на наявність номеру кредитної картки, але без особистих даних, таких як ім'я або банк-емітент. Номер кредитної картки вказує на емітента картки та тип картки. Аналогічно, після того, як жертва повідомила адресу криптовалютного гаманця до правоохоронних органів, за допомогою зовнішніх інструментів є можливості (які не гарантують успіху) співвіднести адресу гаманця до конкретної криптовалюти, конкретного VASP або фінансового посередника. Детальніше про цей процес можна дізнатися з розділу нижче на с. 48: Додаткові інструменти для розслідування злочинів, пов'язаних з віртуальними активами.

9 Інтерпол, Рекомендації щодо арешту віртуальних активів (жовтень 2023 р.), с. 40.

Передова практика для кожного типу транзакцій

Існує три типи трансакцій у блокчейнах, про які важливо знати слідчим, оскільки їм може знадобитися співпраця постачальників послуг віртуальних активів (VASP).

Тип трансакції	Опис	Вплив на розслідування
Обмін фіатної валюти на криптовалюту	Потерпілий здійснив оплату банківським переказом, карткою, мобільним платежем або готівкою в національній валюті до VASP, який обмінює кошти на криптовалюти.	**Практична порада 1** **Спробуйте зупинити або скасувати переказ до криптовалютного брокера, якщо це можливо.** Найбільша помилка на етапі подачі заяви – це реєстрація передбачуваного злочину і призначення співробітника для проведення досудового розслідування. Це затримує початковий контакт з потерпілим. Якщо такої затримки не буде, трансакція потенційно може бути зупинена. Якщо трансакцію було здійснено в неробочий час або у вихідні дні, все ще може бути можливим зупинити здійснення вихідного банківського переказу, оскільки деякі банки обробляють банківські перекази наступного робочого дня. Якщо трансакцію було здійснено за допомогою платіжної картки, можна зв'язатися з емітентом картки, щоб потенційно повернути або зупинити переказ платежу. Ключовий аспект – з'ясувати, яка фінансова установа здійснила банківський переказ. Це буде видно на виписці з банківського рахунку. **Практична порада 2** **Якщо зупинити трансакцію не вдалося, спробуйте визначити, якому постачальнику послуг віртуальних активів (VASP) був відправлений переказ, аби звернутися до нього для зупинки трансакції та заморозки коштів, якщо це можливо.** Якщо криптовалютний брокер працює в країні з низьким рівнем ризику, яка ввела регулювання ПВГ/ПФТ для криптовалютних активів, то є можливість без зволікання звернутися до брокера і запросити заморожування або повернення коштів, якщо вони ще не були обміняні. Іноді цей процес може бути ініційований самими потерпілими. Тоді брокери можуть зупинити обмін коштів, оскільки закони про боротьбу з відмиванням грошей вказують, що кошти можуть бути переказані лише в тому випадку, якщо відомо походження коштів і зрозуміло, куди надсилаються кошти. Повідомлення VASP про те, що криптовалютний гаманець використовується для шахрайства, змусить їх вжити заходів, щоб зупинити його роботу через положення законодавства про відмивання грошей.

Тип трансакції	Опис	Вплив на розслідування
		Хоча це залежить від внутрішньої політики комплаєнсу VASP, тимчасове заморожування коштів на кілька робочих днів дозволить правоохоронним органам або прокурорам подати офіційний запит про повернення коштів. Це можливо, якщо діяти швидко, а криптовалютний брокер належно реагує. Якщо обидва процеси не вдалися, третя можливість полягає в тому, щоб зв'язатися з VASP, який був ідентифікований, і попросити всі докази з їхніх баз даних про особу користувача, який створив обліковий запис користувача (оскільки це, швидше за все, шахрай або фальшива особистість), його ідентифікаційну інформацію та хеш трансакції. (Додаткова інформація про цей процес надана в наступному розділі: інформація криптовалютних брокерів про особу користувачів)
Криптовалюта в криптовалюту	Жертва повідомляє про шахрайство, яке відбувається виключно в технології блокчейну, без зв'язків із традиційними фінансовими службами, які обробляють фіатні валюти. Наприклад, сталося шахрайство, під час якого користувача обманом змусили придбати інший криптовалютний продукт (наприклад, NFT, стейкінг тощо), що призвело до фінансових втрат.	**Практична порада 1** **Шукайте потенційних ліцензованих фінансових посередників, так звані «централізовані біржі», які були задіяні в обміні. Якщо їх вдасться знайти, можливо, вдасться зібрати інформацію про особу залучених сторін через цього посередника.** **Практична порада 2** **Часто постраждалі стають жертвами прийомів соціальної інженерії, які залишають значну кількість кібербезпекових слідів. Наприклад, підозрювані часто просять жертв зв'язатися з ними за допомогою додатків для дистанційного керування, електронних листів, телефонних дзвінків, початкових банківських переказів, СМС або повідомлень комунікатора.** У цьому сценарії жертви зазвичай вже мають досвід роботи з фінансами на основі блокчейну. Початкове завдання полягає в тому, щоб зібрати максимально точну та актуальну інформацію про перекази: час трансакцій, типи валют, які використовують жертви, інформацію про криптовалютні гаманці, квитанції, електронні листи, СМС-підтвердження та інші види інформації. (більш детальну інформацію можна знайти в наступному розділі «Збір доказів»).

Тип трансакції	Опис	Вплив на розслідування
Криптовалюта у фіатну валюту	Потерпілий повідомляє про крадіжку або втрату коштів	У цьому сценарії жертва вже володіла криптовалютами, які були відправлені на біржу криптовалют, а потім обміняні на національну валюту, яка, швидше за все, буде виплачена за допомогою банківського переказу або готівкою у фізичному офісі. Аналогічно із переказами з фіатної валюти на криптовалюту, тут виникає необхідність пошуку фінансового посередника, який провів обмін на національну валюту та ініціював банківський переказ. Якщо задіяні великі надавачі послуг, і фінансова установа розташована в юрисдикції з низьким рівнем ризику, тоді ця установа повинна перевірити, звідки надійшли кошти, і цей крок проводиться вручну співробітниками з комплаєнсу. Якщо такий перегляд відбувається, зазвичай він триває від 24 годин до кількох робочих днів з моменту здійснення трансакції. Якщо можливо, введіть адресу криптовалютного гаманця в провідник блокчейн-гаманця, щоб перевірити її та подивитися, чи підключений він до фінансового посередника, з яким можна зв'язатися (див. розділ «Додаткові інструменти для розслідувачів віртуальних злочинів», стор. 40 для отримання додаткової інформації). Якщо такий пошук не увінчався успіхом, то необхідно використовувати спеціальне програмне забезпечення (постачальника аналітики блокчейну), яке може вказати, чи була адреса підключена до відомої фінансової установи.

Збір доказової бази

Збір доказової бази

Збір інформації від особи

10 типів інформації, що мають вирішальне значення для розслідування

- **Вид активу:** який криптовалютний проєкт або NFT був задіяний, включаючи його назву, символ та специфіку базової технології.
- **Деталі трансакції:** інформація про трансакції, здійснені жертвою, як-от дата, час, сума, валюта та ідентифікатори трансакцій (наприклад, квитанції від VASP).
- **Адреси гаманців:** детальна інформація про адреси криптовалютних гаманців, які використовувалися як жертвою, так і підозрюваним у шахрайстві.
- **Записи спілкування:** будь-яке спілкування жертви з ймовірними шахраями, будь то електронною поштою, соціальними мережами, додатками для чату, телефонними дзвінками або форумом.
- **Рекламні матеріали:** будь-які рекламні оголошення, публікації в Інтернеті або інші рекламні матеріали, пов'язані з віртуальними активами, які були отримані жертвами. У випадку з копіями електронних листів переконайтеся, що в них включені гіперпосилання, в ідеалі на драйверах USB. Попередження! Під час запису такого матеріалу не переходьте за гіперпосиланнями, наданими в електронному матеріалі, оскільки вони можуть бути інфіковані.
- **Дані про платформу:** будь-яка інформація про платформу або біржу VASP (див. розділ «VASPs і CASPs» на сторінці 20), платформу або біржу, на якій жертва придбала криптовалютний актив. Щоб отримати інформацію про те, як запитувати дані від VASP, дивіться розділ нижче, "Запит даних від VASP", с. 29. Назви бірж часто можна знайти на квитанціях про трансакції.
- **Інформація про джерело рекомендації:** інформація про те, як жертва дізналася про актив, будь то через рекомендацію, онлайн-рекламу, сарафанне радіо тощо.
- **Аномалії в коді:** Якщо є, будь-які докази маніпуляцій з кодом, які перешкоджають продажу, або будь-які інші аномалії. Будь-які гіперпосилання на веб-сайти, які використовуються для підтримки злочину, і, залежно від юрисдикції, коли жертва відключила свої фінансові дані, будь-які облікові дані, які допоможуть правоохоронним органам зрозуміти програмне забезпечення.
- **Фінансові записи:** Банківські виписки, виписки з кредитних карток або інші фінансові записи, що показують переказ коштів, пов'язаних з інвестиціями.
- **Ідентифікаційна інформація:** будь-які дані, які можуть допомогти ідентифікувати шахрая, такі як імена користувачів, профілі в соціальних мережах, адреси електронної пошти або будь-яка інша контактна інформація, яка використовувалася під час взаємодії з жертвою на комп'ютері жертви.
- **Технологічні аномалії:** чи встановлювала жертва якісь програмні продукти під час процесу шахрайства? Це програмне забезпечення видалене чи воно все ще на комп'ютері? Чи можна визначити джерело або походження програмного забезпечення?

Якщо криптовалютна трансакція не була призупинена, життєво важливо отримати адресу криптовалютного гаманця, куди або звідки були відправлені або отримані кошти.

Збір адрес криптовалютних гаманців

Яка найважливіша інформація потрібна для розслідування в блокчейні?

Деталі трансакції: адреса криптовалютного гаманця та хеш-номери

Поширеною помилкою є некоректний запис відповідної адреси криптовалютних гаманців, оскільки вони включають довгі рядки цифр і букв.

Приклад 4: При записі адреси криптовалютного гаманця тощо число нуль «0» можна легко сплутати з буквою O, або букву q з g. Найкращою практикою є ввести записану адресу криптовалютного гаманця в пошукову систему Інтернету, наприклад Google або Bing, щоб побачити, чи можна її ідентифікувати. Якщо адреса не з'являється відразу, можна скористатися інструментом провідника гаманця.(див. розділ «Додаткові інструменти для слідчих у справах про віртуальні злочини» на с. 40).

Якщо адреса криптовалютного гаманця вірна, буде миттєво відображатися інформація, яка дозволяє отримати наступні дані:

Завжди для Bitcoin:

- **Сума трансакції:** Ви можете побачити суму Bitcoin, яка була відправлена або отримана в кожній трансакції.
- **Час трансакції:** Видима мітка часу, що вказує, коли трансакція була включена в блок.
- **Поточний баланс криптовалютного гаманця:** Ви можете переглянути загальну суму Bitcoin на даний момент у гаманці.
- **Хеш трансакції:** це унікальний ідентифікатор для кожної трансакції, наприкладідентифікатор трансакції, який використовується постачальниками платіжних послуг, слугуючи його «відбитком пальця».

Доступно в деяких службах, але не в усіх:

- **Розмір трансакції:** Деякі сервіси надають детальну інформацію про розмір трансакції, яку часто відображають в еквіваленті у провідних фіатних валютах, таких як долари США або Євро.
- **Налаштування часового поясу:** деякі платформи пропонують можливість змінювати часовий пояс UTC за замовчуванням. Наприклад, користувачі можуть налаштувати його відповідно до свого місцевого часового поясу, допомагаючи у зборі доказів.

Чи можуть за однією адресою криптовалютного гаманця зберігатися різні типи криптовалют?

Потенційна можливість використання користувачем єдиної програми для доступу до різних віртуальних активів з використанням ідентичних облікових даних втілюються за допомогою гаманця з мультипідписом (MultiSig). MultiSig використовує єдину програму для управління різноманітними віртуальними активами з однаковими обліковими даними, оптимізуючи процес роботи з різними криптовалютами.

Подібно до того, як банки призначають унікальні номери рахунків для різних валют — один для доларів США, інший для євро — криптовалюти на основі різних технологій блокчейну, такі як Bitcoin і Tron, вимагають унікальних адрес гаманців.

Гаманці MultiSig не обов'язково вимагають наявності кількох осіб; натомість, у них використовується кілька приватних ключів для авторизації трансакції. Одна людина може володіти кількома приватними ключами, або кілька осіб можуть бути залучені до управління активами, кожна зі своїм приватним ключем.

Візуалізацію цієї концепції можна порівняти з різницею між типами смартфонів і операційними системами або програмами, які вони підтримують. Деякі програми розроблені виключно для iOS від Apple і вимагають iPhone, тоді як інші адаптовані для Android і не працюватимуть на пристроях Apple. Однак, різні програми, розроблені різними програмістами, можуть працювати на платформі Android і бути отриманим із магазину Google Play. Подібним чином, криптовалютами, об'єднаними загальною технологією, такими як токени ERC20, побудовані на блокчейні Ethereum, можна керувати в межах однієї адреси гаманця на основі Ethereum.

Це відображає те, як єдиний магазин додатків полегшує завантаження численних програм, розроблених на одній платформі. Подібним чином, криптовалюти, розроблені на тому ж блокчейні, як-от Ethereum, можуть бути об'єднані в межах однієї адреси гаманця на основі Ethereum, що забезпечує більш оптимізований користувацький досвід.

Запит даних від постачальників послуг віртуальних активів (VASP)

Якщо жертва не знає, якому постачальнику послуг віртуальних активів (VASP) були відправлені гроші, у неї може бути квитанція із адресами гаманця. Якщо ні, ці дані часто можна побачити за допомогою програмного забезпечення постачальника аналітики блокчейну. Такі провайдери зареєстровані в країнах, де в законах чітко зазначено, що віртуальні активи повинні регулюватися згідно рекомендацій щодо боротьби з відмиванням грошей. Згідно з цими правилами, VASP повинні підтвердити особу своїх користувачів і записувати трансакції. Наприклад, в рамках Європейського Союзу, за даними П'ятої Директиви ЄС про протидію відмиванню коштів, VASP держав-членів ЄС повинні бути зареєстровані та дотримуватися різноманітних зобов'язань щодо боротьби з відмиванням грошей.

Якщо жертва знає, на який VASP були відправлені або звідки прийшли кошти, і все ще має (або може відновити) облікові дані для входу, то першим кроком є вилучення всієї інформації про переказ з біржі. Ця інформація про переказ включатиме проведені трансакції, надіслані криптовалюти та адреси їхніх криптовалютних гаманців.

Якщо потерпілий не впевнений, куди були перераховані кошти або звідки вони були відправлені, назву VASP іноді можна знайти на виписці з банківського рахунку або виписці по картці потерпілого.

Деякі назви віртуальних активів або бірж включають PanCake Swap (https://pancakeswap.finance/); Гаманець Wasabi (https://wasabiwallet.io); Doge Coin (https://dogecoin.com/); і Shit Coin (https://www.investopedia.com/terms/s/shitcoin.asp). Хоча вони не будуть відразу знайомі тим, хто не є активним користувачем у світі криптовалют, вони широко використовуються.

Навіть ті платформи, які стверджують, що вони повністю децентралізовані, такі як Uniswap,

пропонують можливість збереження історії трансакцій для користувачів у .csv, які можуть допомогти у розслідуванні.

У світі існують сотні бірж, і лише кілька назв можуть бути легко впізнаваними для широкої громадськості або правоохоронних органів.

Якщо фізична особа не може отримати доступ до свого облікового запису в VASP, залишається можливість звернутися за допомогою до централізованого VASP або криптовалютного гаманця (до постачальника послуг зі зберігання (custodianship provider)).).

Дотримуючись найкращих практик, VASP зазвичай не надають жодної інформації по телефону, тому існує потреба у запиті правоохоронних органів до VASP або інших фінансових установ, які обробляли обмін коштів жертви. Процес подання ЗПО до VASP описаний на сторінці 22.

Інформація, яку ви, швидше за все, отримаєте від централізованого VASP:

- Ім'я
- Прізвище
- Дата народження
- Копії документів, що посвідчують особу[10]
- Розмір здійснених трансакцій
- Позначка часу трансакцій[11]
- фіатні і криптовалютні трансакції[12]
- Розмір комісії агента
- Час підтвердження перевірки за санкційними списками та списками політично значущих осіб, а також типи списків спостереження, які були використані.
- **Адреса криптовалютного гаманця** або адреси, якщо існує кілька трансакцій і валют
- Хеші трансакцій до проведених трансакцій

Менш вірогідно, але все ж можливо отримати наступну інформацію:

- Номер або ідентифікатор клієнта, зареєстрований у агента
- Задекларована адреса проживання[13] клієнта
- Юридична адреса клієнта[14]
- Номер соціального страхування, залежно від країни, де зареєстрована платформа
- Взаємодія між агентом (VASP/CASP) і клієнтом (часто у форматі PDF, оскільки обслуговування клієнтів часто проводиться зовнішніми постачальниками програмного забезпечення, такими як Intercom або ZenDesk)
- Усі документи, що підтверджують наявність коштів – завантажені користувачами та надіслані їм
- IP-адреса (що може вводити в оману, оскільки користувачі зазвичай використовують VPN)
- Пристрій, що використовується для входу в систему, наприклад мобільний телефон або настільний комп'ютер
- Браузер і версія, що використовується для доступу до сервісу: Opera, Chrome, Safari, Internet Explorer або аналогічна
- Перевірка біографічних даних клієнта, проведена за допомогою Open Source Intelligence (OSINT)[15]
- Коментарі співробітників VASP щодо конкретного користувача або його трансакцій
- Будь-які аналітичні дослідження блокчейну, проведені щодо користувача або його трансакцій співробітниками VASP
- Будь-які запити про конкретного користувача від інших правоохоронних органів або фінансових установ
- Будь-яка трансакція, яка була ініційована користувачем, але не завершена
- У фізичних офісах або банкоматах може бути відеозапис осіб, які користуються приміщенням
- Запитуйте всі документи, які завантажили користувачі (включаючи підтвердження джерела походження коштів і джерела багатства), а також усі взаємодії зі службою підтримки клієнтів

Поліцейські можуть збирати від жертви більше інформації про дані власного банківського рахунку, що допомагає фільтрувати інформацію, зібрану з VASP. Ця інформація буде доступна лише для трансакцій з криптовалюти до криптовалюти (а не для трансакцій між криптовалютою та фіатнj. Валютj.).

- Номер банківського рахунку потерпілого, який використовувався для здійснення переказу на рахунок VASP та з нього.
- Номер телефону: деякі користувачі використовують платіжну систему свого телефону

10 Це може включати паспорт, посвідчення особи або електронне посвідчення особи. Однак цей процес вразливий до тих самих проблем, що й традиційна кіберзлочинність, наприклад, із використанням підроблених або колекційних предметів, які імітують справжні документи, що посвідчують особу (наприклад, «колекційні документи», доступні на таких веб-сайтах, як dokumencik.pl).

11 Важливо визначити, до якого часового поясу відноситься позначка часу. Наприклад, усі трансакції блокчейну Bitcoin реєструються за UTC (за лондонським часом) незалежно від того, звідки походить користувач. Проблема зв'язку неправильних часових позначок трансакцій з іншими доказами іноді була критичною.

12 Як віртуальні активи, так і фіатні валюти.

13 Якщо це дозволено в юрисдикції, можна переглянути, чи є на платформі інші клієнти, зареєстровані за тією ж адресою, які проводили трансакції.

14 Чи витягує платформа таку інформацію з публічної бази даних.

15 Це може включати витяги із загальнодоступних джерел даних, таких як довідки про судимість або інформація про кінцевих бенефіціарних власників конкретних підприємств, які могли бути отримані співробітниками платформи, що відповідають за компдаєнс.

- Інформація з кредитної, дебетової або передплаченої картки, яка використовувалася для трансакції. В обліковому записі постачальника може бути додаткова інформація, наприклад, другий рівень підтвердження через мобільний банківський додаток або або CMC-сервіс "3D secure",

- У країнах, що застосовують принцип прозорого банківського обслуговування, додаткова інформація може бути надана постачальниками платіжних послуг, які проводять такі трансакції (якщо ці трансакції були здійснені за допомогою відкритого банкінгу)

Інформація про формати даних, які можна отримати від VASP

Для оптимальної ефективності рекомендується отримувати необхідні дані про трансакції у форматі «.csv», що сприяє простій інтеграції в правоохоронні системи. Як правило, відповіді на ЗПО надходять у двох форматах:

- «.pdf», в якому VASP надає прямі відповіді на запити, зроблені правоохоронним органом

- Файл ".csv", що містить дані про трансакції

Часто VASP ведуть папки з консолідованими даними про клієнтів. Така папка містить важливі документи, такі як підтвердження коштів (POF) та інші завантажені файли. Великі VASP, як правило, мають встановлений спосіб реагування на запити правоохоронних органів. При взаємодії з невеликими установами правоохоронні органи можуть конкретизувати бажаний формат даних для отримання необхідної інформації.

Однак особистість клієнта іноді може бути записана в різних форматах, таких як «.pdf» або «.jpeg» документа, що посвідчує особу, або відео, яке існує в таких форматах, як «.avi» або «.mov».

Рекомендується утримуватися від запиту файлів ".xml" або ".xls" від VASP. Зокрема, використання файлів «.xlsx» не рекомендується з міркувань кібербезпеки. Існує ризик того, що дані, надані VASP у форматі «.xlsx», можуть містити віруси, особливо в макросах, вбудованих у файл, що може поставити під загрозу безпеку комп'ютерних систем правоохоронних органів.

Надійність отриманих IP-адрес

IP-адресу (Інтернет-протокол (IP)) часто можна отримати від постачальника послуг віртуальних активів (VASP) за запитом правоохоронних органів. IP-адреса – це унікальний ідентифікатор пристрою, як-от смартфон або ноутбук в інтернет-мережі. Подумайте про IP-адресу як унікальний набір цифр, подібний до номеру телефону. Наприклад, 193.46.242.201 вказує на Стокгольм, Швеція. Але так само, як один стаціонарний номер телефону може бути спільним для кількох членів сім'ї в будинку, дякуючи технології під назвою NAT (Network Address Translation), декілька пристроїв можуть використовувати одну IP-адресу.

VASP часто стверджують, що вони можуть експортувати IP-адреси, які були зареєстровані під час входу користувачів, однак надійність цієї інформації для розслідувань повинна ставитись під сумнів. IP-адреси показують лише те, який пристрій отримав доступ до Інтернету, а не хто конкретно ним користувався. Вони можуть бути замасковані шахраями за допомогою віртуальних приватних мереж (VPN), а тому повинні використовуватися лише у випадках, коли є інші докази, які можуть пов'язати IP користувача з потенційною злочинною діяльністю.

Компанії, що надають домашній доступ до Інтернету (так звані інтернет-провайдери), часто можуть ідентифікувати, хто використовував певну IP-адресу в певний час. Під час слідства, таким компаніям може бути запропоновано співвіднести адресу з конкретними користувачами, які підписали договір на їх послуги. На жаль, навіть якщо користувач не використовує VPN, ця інформація не завжди достовірна. Оскільки користувачі можуть надавати доступ до мережі WIFI без паролів, це означає, що можуть бути випадки, коли використовується чужа IP-адреса.

Знання IP-адреси саме по собі не завжди дає точну інформацію про те, хто виконав певну дію в Інтернеті. У таких середовищах, як громадські офіси, школи або на робочих місцях кілька осіб можуть використовувати одне інтернет-з'єднання, що ще більше ускладнює визначення авторства дій в Інтернеті певній особі.

Нарешті, VPN розроблені таким чином, щоб приховувати фактичну IP-адресу користувача, створюючи враження, що з'єднання відбувається з іншого місця. Однак, навіть за допомогою VPN може існувати можливість пов'язати певну поведінку користувача з відвідуванням певних веб-сайтів, пов'язуючи їх з певною IP-адресою протягом певного періоду часу. Це означає, що хоча VPN підвищують анонімність користувача, вони не роблять дії в Інтернеті абсолютно невідстежуваними. За певних обставин все одно існує можливість пов'язувати дії в Інтернеті з окремими користувачами.

Збір IP-адрес

Аргументи «за»:

- **Відстеження:** IP-адреси можуть служити відправною точкою для відстеження потенційних підозрюваних або виявлення джерела підозрілих дій. Є ймовірність, що вони можуть бути пов'язані з іншими розслідуваннями.

- **Стримування:** знання про те, що відбувається моніторинг IP-адрес може стримувати потенційних злочинців від використання власних мереж для незаконної діяльності.

- **Додаткові докази:** у поєднанні з іншими доказами, IP-адреси можуть допомогти побудувати

Роман Бєда проводить практичний семінар для слідчих у Казахстані. Як колишній власник програмного продукту для блокчейн-аналітики та експерт-свідок у судах Європи та Сполучених Штатів, він зосереджується на обміні не лише знаннями, але й найкращими практиками та уявленнями про проблеми, з якими стикаються під час процесу збору доказів. Метою семінарів ОБСЄ є забезпечення того, щоб виклики, з якими стикаються в одній державі-учасниці, не повторювалися в інших.

переконливішу справу проти підозрюваних.

Аргументи «проти»:

- **Неточність:** Оскільки декілька пристроїв можуть використовувати одну IP-адресу, а також через можливості VPN та інших інструментів маскування, покладання виключно на IP-адреси може призвести до невірної ідентифікації.

- **Питання конфіденційності:** Масовий збір IP-адрес може порушувати права приватних осіб, особливо якщо це робиться без належного обґрунтування.

- **Ресурсоємність:** Відстеження та перевірка IP-адрес, особливо коли використовуються VPN або інші інструменти маскування, може зайняти багато часу та відволікати ресурси від інших важливих слідчих дій.

Підсумовуючи, хоча IP-адреси можуть надати додаткову інформацію про активність пристрою та місцезнаходження певного пристрою в певний час, вони не остаточно ідентифікують конкретних користувачів. Розслідування, що ґрунтуються на IP-адресах, корисні лише тоді, коли до них підходили з обережністю і використовували як частину більшого набору інструментів.

Інші документи, які потрібно запитати

У деяких державах-учасницях ОБСЄ компанії, які оперують віртуальними активами (наприклад, криптовалютами), вважаються «зобов'язаними фінансовими установами» або посередниками. Це означає, що вони повинні регулярно контролювати діяльність своїх клієнтів. Вони зобов'язані перевіряти клієнтів і трансакції, які демонструють підозрілу поведінку, часто використовуючи інструменти аналітики блокчейну для виявлення потенційних джерел ризику. Після того, як ці перевірки будуть проведені та задокументовані, правоохоронні органи можуть запросити їх для перегляду.

Наприклад, у Республіці Грузія компанії, що надають обмінні послуги, які зареєстровані в Національному банку Грузії, зобов'язані використовувати спеціалізовані інструменти для аналізу блокчейн-трансакцій. **Це забезпечує рівень прозорості та безпеки під час моніторингу потоку віртуальних активів.**

Якщо правоохоронні органи не мають доступу до таких інструментів аналітики блокчейну, вони можуть звернутися до VASP з проханням надати подробиці для розслідування. Ця інформація може бути в доступному та редагованому форматі, наприклад у форматі PDF або графічному файлі.
Це означає, що, хоча інструменти відіграють важливу роль у підтримці цілісності трансакцій та виявленні незаконної діяльності, існують процедурні та юридичні аспекти, яких слід дотримуватися під час обміну інформацією, отриманою за допомогою цих інструментів. Наприклад, декілька постачальників послуг з аналізу блокчейну та комплаєнсу можуть мати конкретні протоколи та угоди, які обмежують обмін конфіденційною або редагованою інформацією навіть із правоохоронними органами — без попереднього дозволу. Це може створити проблеми щодо готовності VASP розкривати достовірну інформацію на противагу обов'язку обмежувати надання доказів через обмеження угоди.

Передача справ до суду

Передача справ до суду

Прокурори у справах про віртуальні активи

Для того, щоб прокурори мали міцний фундамент для роботи, правоохоронці мають добре розбиратися у зборі доказової бази, пов'язаної з діяльністю по боротьбі з відмиванням грошей, особливо в швидко зростаючій сфері віртуальних активів і криптовалют.

Етап слідства:

- Шукайте цифрові докази: розумійте та контролюйте трансакції на технології блокчейн та розподілених реєстрах.
- Аналізуйте інформацію: виявляйте закономірності, які можуть свідчити про відмивання грошей, такі як швидкі та великі обсяги трансакцій на криптовалютних біржах.
- Шукайте цифрові підказки: відстежуйте потік активів через кілька віртуальних гаманців і платформ, використовуючи спеціалізоване програмне забезпечення, якщо це необхідно.
- Оцініть достовірність всієї ідентифікаційної інформації, отриманої від VASP (див. проблеми з «копіями документів, що посвідчують особу», с. 30)

Підготовка до судового розгляду або слідства

А. Огляд справи:

- Слід зосередитися на криптогаманцях, IP-адресах, мітках часу трансакцій і сумах, якими обмінюються в цифровій сфері.Першим наміром має бути розуміння перетворення віртуальних активів на матеріальні активи, такі як нерухомість або товари, і відстежування їхнього походження.

Б. Визначення виду правопорушення:

- Розпізнайте ознаки криптовалюти, яка використовується для відмивання грошей, наприклад, за допомогою послуг «тмблінгу» або «міксингу», які мають на меті приховати походження коштів. Деякі з провідних постачальників аналітики блокчейну пропонують «деміксінг послуги», стверджуючи, що можуть розбирати трансакції, які були оброблені в міксері. Якщо справа є дуже важливою, існують послуги з деміксингу, які пропонують як постачальники блокчейн-аналітики, так і курси з деміксингу, пропоновані правоохоронними органами, такими як Європол.
- Використовуйте реєстр трансакцій у блокчейні, щоб довести елементи злочину.

В. Зв'язок злочинної діяльності з активами:

- Відстежуйте будь-який рух від криптовалютних гаманців до купівлі матеріальних або інших віртуальних активів. Це може включати дослідження руху криптовалюти з біржі на приватний гаманець, а потім до іншої організації чи послуги.
- Визначте будь-які використані послуги або методи знеособлення та спробуйте відстежити активи, незважаючи на ці проблеми. Розпізнайте закономірності, які можуть вказувати на злочинні наміри, як-от відмивання грошей, наприклад, поділ великих сум криптовалюти між кількома гаманцями або використання монет конфіденційності, як-от Monero або Zcash.

Представлення доказів:

- Наочно поясніть, як працюють криптовалюти і блокчейн, оскільки багато представників судової влади можуть бути не знайомі з цією технологією. Слід представити чіткий і стислий цифровий слід процесу відмивання грошей від джерела незаконних коштів до кінцевого пункту призначення. Рекомендовано створювати візуалізацію та використовувати легку нетехнічну мову під час представлення доказів, оскільки багато прокурорів або суддів можуть ще не повністю бути знайомими зі складнощами криптовалют.

Додаткові докази:

- Записи про криптообмін: вони можуть надавати детальну інформацію про активність користувачів, адреси гаманців, журнали IP-адрес, суми трансакцій і дати.
- Програмне забезпечення для аналізу блокчейну: може візуалізувати потік цифрових валют.
- Перевірка цифрових гаманців: дослідіть апаратні гаманці, мобільні гаманці та настільні гаманці. Вони можуть мати записи, історію трансакцій або метадані, які можуть бути корисними.
- Відстеження IP-адрес: відстеження IP-адрес, пов'язаних з операціями з визначення географічного розташування підозрюваних. (див. п. 31 щодо обмежень IP-адрес)
- Співпраця з міжнародними агентствами: Через децентралізований характер криптовалют міжнародне співробітництво може мати вирішальне значення для відстеження транскордонних трансакцій. Однак така співпраця, як правило, починається на більш пізній стадії старшим слідчим.[16]

Збираючи всебічні докази, пов'язані з криптовалютними трансакціями та діяльністю, поліцейські можуть надати своїм колегам-слідчим, а також прокурорам надійну базу для побудови своєї справи та забезпечення притягнення винних до відповідальності.

16 Підрозділи фінансової розвідки, які працюють разом з Егмонтською групою, розробили механізм системи обміну, доступ до якого можна отримати тут: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (станом на 15 лютого 2024 року)

Рекомендації та контакти для складних справ

Рекомендації та контакти для складних справ

Спеціалізовані колективи експертів та експертні знання

Провідні постачальники програмного забезпечення для аналітики блокчейну часто створюють спеціальні команди, що складаються з експертів як у сфері криптовалюти, так і в розслідувальних процесах. Ці команди спеціалізуються на допомозі правоохоронним органам у тонкощах аналітики блокчейну, забезпечуючи використання інструментів до їх максимального потенціалу. Рекомендується перевірити інтранет вашого агентства, щоб дізнатися, які відділи вже використовують аналітичне програмне забезпечення на основі блокчейну, оскільки колеги в цих відділах, ймовірно, матимуть найкраще розуміння цього питання.

Навчання та сертифікація

Визнаючи складність технологій блокчейну і важливість надійного управління знаннями, багато постачальників програмного забезпечення для блокчейн-аналітики також пропонують структуровані навчальні програми. Ці програми часто завершуються присвоєнням різних рівнів сертифікації, які не тільки перевіряють навички співробітників правоохоронних органів, але й підвищують їх ефективність у проведенні розслідувань, пов'язаних з блокчейном. Хоча деякі послуги, такі як консультаційна підтримка, можуть вимагати додаткового фінансування, довгострокові вигоди з точки зору розширених слідчих можливостей можуть бути значними.

Зовнішня підтримка для поглиблених розслідувань

Крім внутрішніх команд і навчання, розширюється спектр зовнішніх комерційних постачальників, які вміють проводити вичерпні розслідування криптовалютних трансакцій на блокчейні. Ці суб'єкти виступають в якості підрядників, пропонуючи свої спеціалізовані послуги правоохоронним органам. Їхній досвід може виявитися неоціненним, особливо у складних випадках, коли потрібен глибокий аналіз та багатогранні методи розслідування. Правоохоронні органи, такі як Інтерпол або Європол, пропонують спеціальну підтримку та навчання для слідчих (див. розділ «Співпраця з експертами з цифрових активів», с. 52). Якщо ваша команда хоче приєднатися до доступних навчальних заходів, будь ласка, зв'яжіться з VirtualAssets@osce.org для отримання додаткової інформації.

Дійте обережно

Однак, незважаючи на численні переваги зовнішніх постачальників, агентства також повинні усвідомлювати потенційні проблеми. Залучення зовнішніх організацій, таких як консалтингові агентства або постачальники послуг блокчейн-аналітики до конфіденційних розслідувань може ускладнити розгляд справи. Існує також критично важливе питання безпеки даних. До передачі конфіденційної інформації зовнішнім сторонам слід підходити з максимальною обережністю, щоб гарантувати, що цілісність даних збережена і не відбувається ненавмисного витоку конфіденційної інформації.

Мацей Шульц проводить семінар для тренерів у Гданську, на якому політики з держав-учасниць діляться найкращими практиками вирішення складних справ та надання допомоги національним зацікавленим сторонам. Фокус виходить за рамки якості контенту і переходить до ефективних методів реалізації.

Надання підтримки потерпілим

Надання підтримки потерпілим

Потерпілих слід попередити про наступні проблеми:

Жертви одного шахрайства з криптовалютою можуть легко стати жертвами іншого. Організовані шахрайські групи не просто завдають удару один раз, а натомість, націлюються на своїх жертв неодноразово та стратегічно. Нижче наведено подробиці поширених вторинних шахрайств:

- Обман «рятівника»: після початкового контакту особи з шахрайською мережею, інше крило того ж синдикату робить пропозицію, вдаючи з себе професіонала, який може допомогти повернути втрачені інвестиції. Ця, здавалося б, щедра пропозиція має свою ціну: очікується, що жертва заплатить сервісній компанії, щоб повернути втрачені кошти. Після того, як кошти були перераховані, «рятівник» часто зникає разом із втраченими коштами.
- Хитрість «викривача»: В іншій оборудці шахраї можуть видавати себе за незадоволених колишніх співробітників шахрайського підприємства, стверджуючи, що вони мають інсайдерські знання, які нібито можуть допомогти потерпілим повернути свої активи. Процес такий самий, як і з «рятівником» — кошти потрібно сплатити наперед, а потім контактна особа зазвичай зникає.
- Міраж правового захисту: це сценарії, коли до жертв звертається юрист, який обіцяє повернути гроші, особливо коли в гру вступають VASP. Після того, як жертва домовиться про погодинну ставку, ці юристи стверджують, що підготували обширні документи, іноді понад 40 сторінок, які часто детально описують основні наріжні засади законодавства про боротьбу з відмиванням грошей та фінансуванням тероризму, але мають обмежену юридичну цінність. На жаль, шаблони, які використовуються, в основному є загальними і 99% з них залишаються незмінними, тому VASP завалюють тими ж самими документами з невеликими змінами. Жертви отримують непомірно високі рахунки за ці здебільшого зайві зусилля. Важливо усвідомити, що більшість трансакцій VASP є незворотними після того, як вони були виконані. Заяви про «повернення платежів за кредитними картками» мають невеликі шанси на успіх. Отже, такі юридичні дії зазвичай мають низьку цінність і є досить виснажливими для гаманця жертви.

Ольга де Тручіс, експертка ОБСЄ з віртуальних активів та співголова Державно-приватного партнерства фінансової розвідки Європолу (EFIPPP) з питань криптоактивів провела сесію про найкращі практики для традиційних фінансових постачальників у управлінні ризиками фінансових злочинів, пов'язаними з віртуальними активами та постачальниками послуг віртуальних активів. У семінарі, організованому в приміщенні Національного банку Латвії (Latvijas Banka), взяли участь представники чотирьох додаткових держав-учасниць ОБСЄ.

Окремі види злочинів, скоєних з використанням криптовалют

Окремі види злочинів, скоєних з використанням криптовалют

Нижче наведено подробиці про найпоширеніші види злочинів, що вчиняються з криптовалютами. Як мінімум, слід знати про ці види злочинів, але також слід пам'ятати, що це не вичерпний перелік.

Схеми інвестування в криптовалюту

Що це?

Шахрайство з інвестиціями в криптовалюту є одним з найпоширеніших видів шахрайських схем. Спочатку ця афера була націлена на заможних пенсіонерів у країнах з високим рівнем доходу. Однак, ця тактика еволюціонувала, і інвестори фондового ринку та ті, хто наближається до виходу на пенсію, все частіше стають її мішенню. Дуже важливо залишатися пильними та бути уважними до розвитку цієї афери в майбутньому.

Це шахрайство працює так, що шахраї зв'язуються з багатими людьми та пропонують їм вигідні інвестиційні можливості. Як правило, шахрай, видаючи себе за досвідченого криптоінвестора, звертається до людей, які нічого не підозрюють і володіють значними статками.

Різні види цієї афери

Зазвичай існують різні види оборудок:

- **Авансові комісії:** Шахраї заманюють людей обіцянкою високого прибутку від інвестицій. Однак для того, щоб почати процес, вони вимагають сплатити внесок, від 250 до 1000 євро (або еквівалент у відповідній національній валюті), як правило, на нижній межі цього діапазону. Отримавши цей початковий платіж, шахрай просто зникає, залишаючи потерпілого із фінансовими втратами та без перспективних інвестицій.
- Більш складний підхід включає відеодзвінок у прямому ефірі, під час якого шахрай демонструє «фінансовий рахунок», який, як стверджується, належить майбутній потерпілій особі, на який відбувається значний приплив грошей. Хоча ці облікові записи розроблені так, щоб виглядати справжніми, вони насправді є копіями дизайну і не мають жодного зв'язку з традиційними фінансовими установами.
- Іноді жертви отримують «першу виплату» в розмірі, наприклад, від 50 до 100 євро, які шахраї називають відсотками на їхні інвестиції, щоб спонукати жертву заплатити більше.
- **Крадіжка особистих даних:** щоб створити ілюзію легітимності, шахраї можуть запитати особисті ідентифікаційні дані жертви нібито для переказу коштів або депозитів. Однак замість того, щоб допомогти в інвестиціях, вони отримують несанкціонований доступ до особистих та фінансових даних потерпілого. Жертви забувають заблокувати свої документи, що посвідчують особу у фінансовій установі, або навіть надсилають копії цієї інформації шахраю.

Як з цим боротися

- **Не здійснюйте жодних додаткових переказів.** Часто шахраї говорять про невеликі витрати на переказ або на виплати, які здаються дуже маленькими в порівнянні із загальною сумою шахрайства. Приклад: комісія в розмірі 600 євро за шахрайство на суму 60 000 євро.
- **Жертва не повинна припиняти контакт.** Як правило, до того моменту, коли потерпілий звертається до правоохоронців, його контакт з аферистом вже розірваний. Але якщо це не так, то слідству може допомогти збереження контакту потерпілим, щоб уможливити пошук інструментів кіберзлочинності, які використовуються.
- **Жертви не повинні** видаляти будь-яке програмне забезпечення, яке було встановлене на їхніх

Користувачам, які менш досвідчені в інвестиціях, фінансах або використанні онлайн-інструментів, шахраї часто встановлюють програмне забезпечення віддаленого доступу.

Це програмне забезпечення в першу чергу призначене для віддаленого доступу, контролю і підтримки. Воно дозволяє користувачам віддалений доступ і управління своїм настільним комп'ютером, ноутбуком або сервером з будь-якого місця. Потерпілий часто сам встановлює таке програмне забезпечення за допомогою шахрая. Після того, як зв'язок було встановлено, жертви часто забувають видалити програмне забезпечення. Сліди, що залишає по собі програмне забезпечення, можуть стати в нагоді для розслідування правоохоронними органами, якщо їх правильно зберегти.

Залежно від типу програмного забезпечення існують різні типи функцій, зокрема:

- **Дистанційне керування:** користувачі можуть керувати комп'ютером з іншого місця так, ніби вони сидять перед ним. Це корисно для ремонту, віддаленої технічної підтримки, або доступу до файлів.
- **Передача файлів:** Програмне забезпечення, яке надає користувачам можливість передавати файли між комп'ютерами. Це іноді призводить до встановлення «кілогера» – шпигунського ПЗ, яке моніторить те, що друкує користувач, та може ділитися цими даними зі злочинцями впродовж років після встановлення на комп'ютері.
- **Віддалений доступ:** це дозволяє шахраям отримати віддалений доступ до комп'ютера або сервера жертви, а також змінювати файли, інсталювати програми або ініціювати підключення.
- **Мобільний доступ:** ця функція забезпечує дистанційне керування приладами зі смартфонів та планшетів.

пристроях, оскільки воно може залишити кібер-сліди, корисні для розслідувань. Однак, жертва повинна знати про можливість наявності на своєму пристрої програмного забезпечення, яке відстежує, що вона друкує, або яке тримає камеру увімкненою тощо. Якщо це так, потерпілий повинен обмежити використання свого пристрою.

- **Перевірте, яку особисту інформацію було оприлюднено.** Якщо є можливість, змініть логіни банків та замовте нові паролі для інструментів електронної ідентифікації, якщо такі інструменти використовуються.
- **Перегляньте розділ про вторинні шахрайства** — детальніше на с. 38.
- **Відповідні заходи, які слід вжити, залежать від конкретних обставин потерпілого.** Для отримання додаткової інформації, будь ласка, зверніться до розділу «Найкращі практики для кожного типу трансакцій» на сторінці 24.

Ще одним поворотом у цій афері є використання фальшивих рекомендацій від знаменитостей. Шахраї привласнюють реальні фотографії та поєднують їх із сфабрикованими акаунтами чи рекламними матеріалами, створюючи враження, ніби відомі особистості підтримують цю схему.

Вимагання і секс-шантаж

У випадках вимагання особи часто отримують добре підготовлений електронний лист, у якому неправдиво повідомляється, що хакер отримав доступ до комп'ютера жертви та може підключитися до камери ноутбука чи смартфона.Коли справа доходить до сексуального шантажу, він зазвичай полягає в тому, що хакер стверджує, що зняв жертву на відео під час акту мастурбації.

Що це?

Фізична особа отримує електронний лист від шахрая. У цьому електронному листі йдеться про те, що шахрай зламав комп'ютер або смартфон жертви та отримав доступ до камери. У випадках сексуального вимагання шахрай стверджує, що записав кадри з жертвою під час акту мастурбації та опублікує відео, якщо жертва не заплатить їм у криптовалюті.

Жертві пропонується переказати кошти на вказаний криптовалютний гаманець у стислі терміни, аби перешкодити оприлюдненню таких нібито відзнятих матеріалів діловим та приватним контактам, які, як стверджує хакер, він знайшов на пристрої. Як «доказ» своїх тверджень, хакер зазвичай надає список імен користувачів і паролів, пов'язаних із різними веб-сайтами, припускаючи, що жертва використовувала ідентичні облікові дані на кількох сайтах із вмістом для дорослих.

Оригінальне електронне повідомлення, надіслане автору цієї публікації:

Тема: Я вас записав – (тут шахрай передає пароль, який отримав при зламі)
Дата: 2023-06-22 3:32
Відправник: "Врятуй своє життя" <xxxxxxxxxf@xxxx.ga>
Отримувач: XXXXXX@xxxx.com

Привіт, я хакер і програміст, я знаю один з ваших паролів: (пароль користувача, отриманий при зламі системи)

Ваш комп'ютер був заражений моїм особистим шкідливим програмним забезпеченням, тому що ваш браузер не був оновлений, у такому випадку достатньо просто відвідати якийсь веб-сайт, де розміщено мій iframe, щоб автоматично отримати вірус, якщо ви хочете дізнатися більше – Google: "Drive-by exploit".

Моє шкідливе програмне забезпечення надало мені повний доступ до всіх ваших облікових записів (див. пароль вище), повний контроль над вашим комп'ютером, і я зміг шпигувати за вами через вашу веб-камеру.

Я зібрав всі ваші особисті дані, записав кілька відео з вами (через вашу веб-камеру) і я ЗАПИСАВ, ЯК ВИ ЗАДОВОЛЬНЯЄТЕ СЕБЕ!!

Я можу опублікувати всі ваші приватні дані скрізь, включаючи даркнет, де знаходяться дуже хворі люди, і відео з вами, відправляти їх вашим контактам і викладати в соціальні мережі і в інших місцях!

Тільки ви можете перешкодити мені це зробити, і тільки я можу вам допомогти. Слідів не залишилося, оскільки я видалив своє шкідливе програмне забезпечення після того, як моя робота була виконана, і цей електронний лист(и) був відправлений з якогось зламаного сервера...

Єдиний спосіб мене зупинити – заплатити рівно 400$ у Bitcoin (BTC).
Це дуже хороша пропозиція, порівняно з усім тим ЖАХЛИВИМ лайном, яке станеться, якщо ви не заплатите!
Ви можете легко купити Bitcoin тут: www.xxxxxxx.com www.xxxxx.com, www.xxxxxx.com або перевірити наявність Bitcoin банкомату поруч з вами або погуглити для інших бірж.

Ви можете відправити Bitcoin прямо на мій гаманець або спочатку створити свій власний гаманець тут:
www.login.xxxxx.com/en/#/signup/, потім отримати і відправити на мій.
Мій біткоін гаманець: **17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG**
Скопіюйте та вставте його; це (cAsE-sEnSEtiVE). У вас є 3 дні.

Оскільки я отримав доступ до цього облікового запису електронної пошти, я знатиму, чи був цей лист прочитаний.

Якщо ви отримуєте цей лист кілька разів, це для того, щоб переконатися, що ви його прочитали, скрипт мого поштовика налаштований так, а після оплати ви можете його проігнорувати.

Після отримання платежу я видалю всі ваші дані і ви зможете спокійно жити своїм життям, як раніше. Наступного разу оновіть браузер перед переглядом веб-сторінок!

Ніна-Луїза Сідлер у Ризі проводить семінар для політиків п'яти держав-учасниць, ділячись висновками круглих столів з регулювання віртуальних активів. Сесія була зосереджена на загальноєвропейському законодавстві, пов'язаному з віртуальними активами, з метою виявлення недоліків у регулюванні та висвітлення нових подій, що мають значення для держав-учасниць.

Як з цим боротися

Найкращі практики підтримки жертв, які повідомляють про електронні листи з вимаганням.

- **Зберігайте спокій:** якщо користувач отримав електронний лист, що містить сексуальні вимагання, необхідно зберігати спокій. З наведеного вище прикладу електронного листа видно, що злочинці використовують сильні прикметники, з метою вселити страх, створити відчуття нагальності і викликати сором, а також паніку.

- **Жертва не повинна взаємодіяти** з відправником у будь-який спосіб: електронні листи із сексуальним вимаганням зазвичай не надсилають нічого як доказ або не містять вкладень. Якщо разом з електронною поштою надіслано будь-які посилання, користувач не повинен їх відкривати.

- Користувачеві має бути заборонено обмінювати фіат на криптовалюту та переказувати його на підозрілий криптовалютний гаманець.

- **Верифікація криптовалютного гаманця:** один із способів оцінити автентичність адреси криптовалютного гаманця = використати інструменти, які зазвичай називають «провідниками гаманців». Наприклад, згаданий криптовалютний гаманець можна дослідити за наступним посиланням:

  https://www.blockchain.com/explorer/addresses/btc/17yshaYmvdp4yjU-3WoCwowh6HHjTfEGDuG.

- При первинному дослідженні, яке залишається безкоштовним і займає менше 10 секунд, стає очевидним, що цей гаманець отримав кілька трансакцій. Це часто суперечить заяві хакера про те, що це унікальна і одноразова адреса криптовалютного гаманця. Численні трансакції свідчать про те, що на нього могли переказати кошти кілька осіб.

- **Використання ринку викрадених облікових даних на користь жертв:** Жертви можуть використовувати безкоштовні послуги, такі як: https://haveibeenpwned.com, які дозволяють їм перевірити, чи не були їхні дані вразливі до витоку даних, прочісуючи мільярди витоків інформації про реквізити рахунків. Вводячи свою електронну пошту або ім'я користувача, користувачі можуть побачити, чи відображається їхня інформація в будь-яких відомих порушеннях. Якщо зловмисник надіслав вам ваш пароль, який реально використовується, негайно змініть його на всіх платформах, де він використовується.

Під час здійснення слідчих дій щодо осіб, підозрюваних у вимаганні, відстеження платежів на їхні криптовалютні гаманці має важливе значення.

Якщо це зробити, можна побачити, чи не прив'язані якісь гаманці до офіційних фінансових платформ, що може допомогти правоохоронним органам визначити, хто надсилав гроші підозрюваному. Хоча оплата на гаманець здирника не є злочином, ті, хто це зробив, могли мати відповідну інформацію або стикатися з подібними погрозами від однієї і тієї ж особи, що може допомогти розслідуванню.

У Секретаріаті ОБСЄ у Відні проводяться тренінги для українських політиків щодо прогалин у регулюванні віртуальних активів з акцентом на децентралізовані біржі.

Шахрайські схеми з раптовим виведенням коштів («rug pull»)

Шахрайство з виходом, шахрайство з накачуванням і скиданням або шахрайство з «висмикуванням килима» (згідно метафори «висмикування килима з-під когось») — це схеми, в яких шахраї створюють багато ажіотажу навколо нового цифрового активу. Це може бути будь-який тип цифрового активу, а не лише нова криптовалюта. Такі шахрайства були виявлені з проєктами та взаємозамінними токенами (NFT). Потім шахраї швидко залишають проєкт, викрадаючи гроші інвесторів і знецінюючи цифровий актив до нуля.

Що це?

Мета цього виду шахрайства полягає в тому, щоб залучити якомога більше покупців або інвесторів для нового цифрового активу, а також якомога більше штучно завищити його вартість. Як тільки шахраї зібрали достатню кількість грошей, вони зникають («вихід» з афери) і забирають гроші собі. Цей вихід може статися швидко, з раптовим зникненням усіх контактів, або з часом, коли гроші повільно виводяться з афери і злочинці навмисно сповільнюють залучення нових осіб. У такому випадку, іноді буває важко відрізнити справжнє шахрайство з «висмикуванням килима» від просто погано реалізованого, невдалого проекту.

У будь-якому випадку вихід шахраїв означає, що актив виявляється фальшивим і втрачає вартість. Жертвам залишається або кілька монет, або токени, які коштують невелику частину того, що вони за них заплатили, якщо вони зможуть знайти покупця, або цифровий актив містить код, який вказує, що актив взагалі не можна продати.

Фішингові шахрайські схеми

Фішингове шахрайство широко поширене в Інтернеті. Це також поширений і ефективний вид шахрайства, пов'язаний із цифровими активами.

Що це?

Шахраї вдають, що представляють офіційний бізнес із законними веб-сайтами чи корпоративними документами і розсилають тисячі електронних листів і повідомлень з посиланнями, що ведуть до їхньої фальшивої версії веб-сайту. Цей веб-сайт створено, щоб дозволити вхід і зберігати особисту інформацію кожного відвідувача, а також усі криптоадреси та паролі (так звані «ключі криптогаманця»), які вони вводять. Це особливо важливо для криптозлочинів, оскільки, на відміну від інших видів облікових записів, якщо приватний ключ криптогаманця вкрадено, то обліковий запис майже неможливо відновити. Це означає, що кошти в гаманці втрачаються назавжди.

Різні види шахрайства

Згідно зі звітом, опублікованим одним постачальником блокчейн-аналітики, 17 нові типи фішингових шахрайств передбачають розігрування карти «страху помилитися» у нових криптоінвесторів, змушуючи жертв надсилати гроші не на той рахунок у надії купити NFT. Це означало, що жертви втрачають лише суму грошей, яку вони надіслали не на той рахунок, а не весь гаманець.

Ще однією варіацією шахрайства, що набирає популярності, є «отруєння адреси», при якому шахрай створює адресу, схожу на ту, на яку потенційна жертва раніше надсилала кошти. Потім шахрай надсилає невелику суму криптовалюти жертві, сподіваючись, що вона мимоволі здійснить наступний платіж на ту саму шахрайську адресу замість легального одержувача.

17 Звіт про незаконну криптоекосистему. (2023), доступний за посиланням: https://www.trmlabs.com/report (дата звернення: серпень 2023 р.).

Що можна зробити, щоб цього уникнути?

Люди повинні знати про фальшиві фішингові посилання та перевіряти всі посилання.

Ретельно перевіряйте адреси:

- Завжди перевіряйте ще раз адресу, на яку ви надсилаєте кошти, особливо коли маєте справу з великими сумами. Не покладайтеся виключно на функції буфера обміну (так звана функція копіювання-вставки), оскільки зловмисне програмне забезпечення може маніпулювати ними, щоб вставити адресу криптовалютного гаманця, відмінну від тієї, яку, на думку жертви, вона скопіювала.
- Використовуйте закладки для часто відвідуваних криптосайтів. Це дозволяє уникнути ризику неправильного введення тексту або потрапляння на фішинговий сайт, який виглядає схоже.

Увімкніть додаткові заходи безпеки:

- Рекомендується використовувати двофакторну аутентифікацію (2FA) скрізь, де можливо. Це додає додатковий рівень безпеки, що ускладнює шахраям доступ до облікових записів.
- Регулярно оновлюйте та запускайте антивірусне програмне забезпечення, щоб виявляти та видаляти потенційні загрози на своєму пристрої. Деякі віруси призначені для моніторингу криптовалютних трансакцій або для зміни даних буфера обміну.

Використовуйте менеджери паролів: менеджери паролів – це програмні інструменти, призначені для зберігання, керування та автоматичного заповнення паролів. Вони також часто дозволяють користувачам створювати безпечні нотатки, які можуть надійно зберігати номери криптовалютних гаманців для різних облікових записів в Інтернеті.

Атаки посредника («людина посередині»)

Що це?

У цьому типі шахрайства шахраї не націлюються безпосередньо на жертву, а натомість перехоплюють передачу даних коли хтось отримує доступ до свого криптовалютного облікового запису в загальнодоступній або незахищеній мережі Wi-Fi, тобто там, де відвідані веб-сайти та інформація, що надсилається з комп'ютера на веб-сайт, не є конфіденційною. Шахраї збирають адресу криптогаманця, дані для входу та ключі від гаманця, а потім використовують це, щоб заволодіти обліковим записом.

Як з цим боротися або уникнути?

Цього типу шахрайства можна уникнути за допомогою віртуальної приватної мережі (VPN). Вони досить дешеві, зазвичай лише від 3 до 4 євро на місяць. VPN шифрують з'єднання користувача з Інтернетом, що ускладнює несанкціонованим особам доступ до інформації про веб-сайти, які відвідуються, або про дані, що вводять. Це також приховує оригінальну IP-адресу користувача, дозволяючи анонімно переглядати веб-сторінки та запобігаючи визначенню фактичного географічного розташування користувача. Це дозволяє користувачам мати віддалений доступ до ресурсів своєї організації або обходити цензуру.
(Детальніше див. у розділі про збір IP-адрес на стор. 31)

Підробні сайти, що імітують криптовалютні біржі

Що це?

Замість того, щоб створювати фальшиву криптовалюту, шахрай створює веб-сайти, схожі на криптовалютні біржі. Коли жертва переходить на цей веб-сайт, щоб обміняти свій тип криптовалюти на інший, або на фіатну валюту, шахраї викрадають їхні дані та внесену криптовалюту.

Як з цим боротися або уникнути?

Щоб підвищити безпеку, завжди використовуйте двофакторну автентифікацію (2FA) під час входу на вашу біржу. Цей додатковий рівень перевірки може включати отримання одноразового коду через СМС або електронну пошту, який вам потрібно ввести під час входу в систему. Крім того, якщо держава-учасниця ОБСЄ пропонує рішення для електронної ідентифікації, розгляньте можливість використання його для додаткового захисту під час входу в систему.

Вторинні шахрайські схеми

Існують також вторинні шахрайські схеми, які виникають після того, як жертву вже обдурили в минулому. Вони висвітлені в розділі «Підтримка потерпілого» на с. 37.

Зліва направо: Марчін Зараковскі, Міхал Громек, Анна Паєвська та Ніна-Луїза Сідлер, які провели незалежний семінар, присвячений викликам та перевагам нагляду за постачальниками послуг віртуальних активів (VASP), для української делегації. У засіданні взяли участь представники ключових українських установ, таких як Національний банк України (НБУ), Державна служба фінансового моніторингу України (Держфінмоніторинг), Міністерство цифрової трансформації та Національна комісія з цінних паперів та фондового ринку (НКЦПФР). Семінар відбувся у Міністерстві фінансів Польщі, яке з щедрістю продовжує безкоштовно надавати свої приміщення для серії тренінгів для українських делегатів.

Додаткові інструменти для розслідування злочинів у сфері віртуальних активів

Додаткові інструменти для розслідування злочинів у сфері віртуальних активів

Інструменти блокчейн-аналітики

Хороший інструмент блокчейн аналітики або провідник гаманця означає, що поліцейські можуть проводити частину розслідувань без необхідності покладатися на інформацію від VASP, яка може бути повільно наданою або неповною. Крім того, ще не всі VASP використовують інструменти блокчейн. аналітики

Чому це важливо:

Правоохоронні органи часто запитують інформацію про поточний баланс конкретної адреси криптовалютного гаманця від VASP. У той час як команди VASP з комплаєнсу оснащені для того, щоб відповідати на ці запити, підготовка відповідей створює значне адміністративне навантаження. Більш ефективною альтернативою є введення адреси криптовалютного гаманця в провідник гаманця, який потім швидко надає необхідну інформацію для більшості, але не всіх провідних криптовалют.

Інформація, яку пропонують оглядачі гаманців:

- Поточний баланс у криптовалюті та основних фіатних валютах, наприклад, доларах США.
- Загальна сума коштів, отриманих криптовалютним гаманцем.
- Загальна сума коштів, відправлених з криптовалютного гаманця.
- Позначки часу для трансакцій. (Примітка: час трансакції може відрізнятися залежно від часового поясу криптовалюти).
- Комісії, що стягуються на блокчейні.
- Джерело: адреси криптовалютних гаманців (звідки були переведені кошти).
- Адреси криптовалютних гаманців призначення (на які були відправлені кошти).

Для тих, хто не знайомий з аналітикою блокчейну, ці дані можуть здатися поверхневими. Однак, для розслідувальних цілей вони можуть надати цінну інформацію, наприклад, виявити закономірність багатьох невеликих вхідних трансакцій у поєднанні з меншою кількістю великих вихідних трансакцій. Такий тип картини може натякати на діяльність, схожу на діяльність торговця наркотиками.

Приклади з реального світу:

Встановлено, що у кримінальних справах використовувалися такі гаманці:

- Криптовалютний гаманець пов'язаний зі справою про секс-шантаж: Blockchain Explorer
- Криптовалютний гаманець, пов'язаний з Twitter Hack, провідником гаманців, який збирає відгуки від користувачів, і Chain Abuse

Як і до всіх відкритих джерел інформації, до будь-яких даних, отриманих від таких провідників слід підходити зі скепсисом і перевіряти їх, перш ніж робити будь-які висновки.

Приклади безкоштовних інструментів блокчейн аналітики:

- Block Explorer: Це простий інструмент, який надає детальну інформацію про блоки, адреси та трансакції Bitcoin. Це хороша відправна точка для початківців.
- Etherscan: Цей інструмент розроблений спеціально для блокчейну Ethereum і може запропонувати детальну аналітику трансакцій та адрес.
- Blockchair: Цей інструмент охоплює кілька блокчейнів, від Bitcoin до Ethereum, що робить його універсальним для тих, хто хоче аналізувати різні мережі.

Ольга де Тручіс та Грета Баркаускієне, експерти ОБСЄ з віртуальних активів і співкерівники напряму "Криптоактиви" в рамках державно-приватного партнерства з фінансової розвідки Європолу (EFIPPP), взяли участь у пленарному засіданні EFIPPP у квітні 2024 року в штаб-квартирі Європолу в Гаазі. Разом вони сприяли проведенню сесій з обміну знаннями, під час яких учасники з різних країн, включаючи країни-бенефіціари ОБСЄ, досліджували та обговорювали нові способи діяльності організованої злочинності у сфері віртуальних активів.

Постачальники блокчейн-аналітики

Постачальники аналітики блокчейну є комерційними аналогами дослідників гаманців.

Вони використовують спеціалізоване програмне забезпечення, призначене для моніторингу, аналізу та візуалізації діяльності в блокчейн-мережах. Ці інструменти допомагають слідчим виявляти закономірності, стежити за трансакціями та отримувати уявлення про величезний і складний світ блокчейну.

Окрім даних, доступних за допомогою провідника гаманця, постачальники аналітики блокчейну пропонують:

- **Відстеження:** Більшість інструментів аналітики можуть відстежувати шлях криптовалютної трансакції від її джерела до місця призначення. Це життєво важливо для розуміння потоку коштів та виявлення будь-якої потенційної незаконної діяльності.
- **Візуалізація:** ці інструменти часто пропонують візуальні схеми та діаграми, щоб полегшити розуміння великих обсягів даних з першого погляду та підключення криптовалютних гаманців до фінансових установ або пов'язування трансакцій з постачальниками гаманців.
- **Оцінка ризиків:** аналізуючи моделі трансакцій, деякі інструменти можуть оцінювати ризик, пов'язаний з конкретними гаманцями або трансакціями, пропонуючи цінну інформацію для фінансових установ і регуляторів.
- **Комплексні дані:** ці інструменти можуть отримувати та інтегрувати дані з різних блокчейнів, надаючи користувачам цілісне уявлення про криптовалютний ландшафт, що може бути корисним для більшої кількості розслідувань.
- **Послуги деміксингу:** деякі провайдери стверджують, що їхні сервіси здатні відображати трансакції між міксерами та тумблерами, які є послугами, призначеними для підвищення конфіденційності та анонімності криптовалютних трансакцій. Дивіться розділ про міксери та тумблери для отримання додаткової інформації. (Перегляньте також інформацію про послуги з деміксування на с. 20)

Використовуючи ці інструменти, дослідники можуть краще розуміти складну динаміку світу блокчейну, забезпечуючи обґрунтовані рішення та більш глибоке розуміння цієї революційної технології.

Протягом двох років експерти ОБСЄ з віртуальних активів надавали важливу підтримку групі експертів з віртуальних активів у головному відділенні Національного банку Грузії. У результаті цього позиція Грузії в рейтингу MONEYVAL підвищилася до "Значною мірою відповідає" (Рекомендації №15 ФАТФ).

Співпраця з експертами з цифрових активів

Співпраця з експертами з цифрових активів

Під час роботи з цифровими активами та пов'язаними з ними повідомленнями на дільницях правоохоронних органів, співпраця із зовнішніми організаціями набуває особливої важливості. До таких утворень належать міжнародні поліцейські організації, банки та спеціалізовані підрозділи в межах певних країн. Їхній досвід допомагає ефективно проводити розслідування.

Пошук місцевих експертів

Вкрай важливо виявляти місцевих представників правоохоронного органу, які мають досвід роботи з віртуальними активами. Наявність їхніх контактних даних може бути корисною з наступних причин:

- **Мета:** Ставити запитання та отримувати інсайти під час процесів звітності.
- **Приклад:** Національне агентство боротьби зі злочинністю Великої Британії (NCA) створило спеціальний криптопідрозділ, який може надавати експертну підтримку у складних справах. Натхнення для організації співпраці в правоохоронних органах щодо віртуальних активів також можна знайти у Звіті про типології за 2023 рік, складеному Радою Європи.[18]

Міжнародна підтримка

Платформа Європолу для експертів (EPE):

- **Опис:** Це безкоштовна платформа для практичної допомоги щодо віртуальних активів для представників правоохоронних органів.
- **Вимоги до кандидатів:** Щоб мати право на отримання підтримки від EPE (https://epe.europol.europa.eu/), держава повинна бути членом Європейського Союзу або бути частиною так званої оперативної угоди.[19]
- **Переваги:** EPE пропонує найкращі практики щодо розслідувань у сфері віртуальних активів. Вона забезпечує доступ до вебінарів, а також контактні дані зацікавлених сторін, конференцій та інших навчальних ресурсів.
- **Процес приєднання:** Якщо держава-учасниця ОБСЄ є частиною оперативної угоди[20] Будапештського меморандуму (список надається окремо), вона може подати заявку на доступ. Процес складається з наступних кроків:
  - Зверніться до призначеного органу за адресою o3 (at) europol.europa.eu за допомогою робочого електронного листа і вкажіть, що пов'язує вас із віртуальними активами та як ваші знання принесуть користь іншим.
  - Чітко зазначте причини приєднання, зокрема щодо віртуальних активів.
- **Хто може долучитися:** Хоча платформа в першу чергу призначена для співробітників правоохоронних органів, до неї також можуть долучитися експерти поза цим колом, як державні, так і приватні. Однак деталізація доступної інформації може бути обмеженою для фахівців, які не є представниками правоохоронних органів.
- **Вартість:** Комісія не стягується. Доступ повністю вільний.

У жовтні 2019 року Європол запустив дві освітні ігри під назвою «Криптопол». Вони оновлювалися декілька разів і містять сценарії щодо декількох криптовалют. Вони залишаються безкоштовними для агентів з країн-членів ЄС. Див.: o3@europol.europa.eu.

18 Див. "Добірки справ" ("Case Boxes") – Звіт про типології за 2023 рік – Ризики відмивання грошей та фінансування тероризму у світі віртуальних активів, Moneyval, Рада Європи https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 (станом на 25 лютого 2024 року).

19 Угоди та робочі домовленості з країнами. Європолу https://www.europol.europa.eu/partners-collaboration/agreements (станом на 26 листопада 2023 р.).

20 Угоди та робочі домовленості з країнами. Європолу https://www.europol.europa.eu/partners-collaboration/agreements (станом на 26 листопада 2023 р.).

Центр Інтерполу з питань боротьби з фінансовими злочинами та корупцією (IFCACC)

Центр Інтерполу боротьби з фінансовими злочинами та корупцією (IFCACC): Це центр, який займається протидією транснаціональним фінансовим злочинам та має на меті захист глобальних фінансових систем.

Відповідність вимогам: У відповідь на зростаючу стурбованість глобальними фінансовими злочинами, Інтерпол запровадив IFCACC як консолідований засіб реагування на допомогу в боротьбі з цими викликами. Це виходить за рамки простої правоохоронної роботи, а також стосується міжнародних органів та зацікавлених сторін.

Переваги: IFCACC сприяє:

- Боротьбі з шахрайством, злочинах з платіжними системами та наданні відповідей на транскордонні запити від правоохоронних органів.
- Боротьбі з відмиванням грошей, поверненні активів та розумінні віртуальних активів.
- Забезпеченню контролю за антикорупційними практиками, від питань, пов'язаних зі спортом, до політичних розбіжностей на високому рівні.

Процес приєднання: Оскільки IFCACC працює за міжвідомчою моделлю, потенційна співпраця включає:

- Встановлення контакту з Генеральним секретаріатом Інтерполу або з Національним центральним бюро Інтерполу, яке зазвичай підпорядковується Міністерству юстиції держави та національній поліції.
- Демонстрація чіткого узгодження цілей у боротьбі з фінансовими злочинами та корупцією.
- Окреслення потенційних сфер співпраці або потреб.

Хто може долучитися: окрім правоохоронних органів, фінансові установи, міжнародні організації та представники приватного сектору можуть співпрацювати із IFCACC. Однак, глибина співпраці може варіюватися залежно від характеру та мети об'єднання.

Вартість: Оскільки Інтерпол є міжнародною організацією, взаємодія з його Генеральним секретаріатом не передбачає жодних витрат.

Для отримання додаткової інформації про IFCACC та I-GRIP див.:

- IFCACC@interpol.int
- IGRIP@interpol.int

Для отримання додаткової інформації, пов'язаної з технічними аспектами віртуальних активів, співробітники правоохоронних органів можуть надіслати електронний лист на адресу: innovation@interpol.int

Додатковий ресурс: співробітники правоохоронних органів можуть запросити Рекомендації Інтерполу щодо арешту віртуальних активів: vaguidelines@interpol.int

Програми УНП ООН щодо віртуальних активів, спрямовані на боротьбу з кіберзлочинністю та відмиванням грошей, і семінари з розслідування

Огляд:
Очолювана командою Управління ООН з наркотиків і злочинності (UNODC), ця всеосяжна серія семінарів пропонує глибоке вивчення віртуальних активів, фінансових злочинів і ключової сфери комплаєнсу.

Навчальна програма поділена на базові, поглиблені та каскадні сесії, які визначаються як навчання тренерів, останні заохочують поширення найкращих галузевих практик. Семінари поєднують жорсткі теоретичні конструкції з практичними вправами, озброюючи представників правоохоронних органів безцінними навичками відстеження, розслідування та вмілого управління віртуальними активами.

Доступ:
Цей спеціалізований тренінг призначений для професіоналів у різних секторах, таких як правоохоронні органи, фінансові установи, технологічні підприємства та освітні галузі. Він є безцінним ресурсом для політиків, регулюючих органів, слідчих і всіх фахівців, які мають намір розібратися у складнощах віртуальних активів, динаміці блокчейну та мистецтві боротьби із фінансовими злочинами.

Основні напрямки роботи:

- **Основні відомості про віртуальні активи:** Заглиблення в генезис, еволюцію та складні аспекти віртуальних активів, що постійно розвиваються, та технологій, що лежать у їх основі.
- **Динаміка трансакцій:** розшифровка життєвого циклу трансакцій блокчейну від початку до кінця.
- **Поглиблений блокчейн:** розкриття процесів, за допомогою яких транзакції реєструються, ратифікуються та архівуються в блокчейні.
- **Криміналістика блокчейну:** Отримання навичок спостереження за трансакціями в режимі реального часу та виявлення схем, які використовують зловмисники для приховування своєї особистості.
- **Тактика протидії відмиванню коштів та фінансуванню тероризму:** засвоєння навичок із забезпечення відповідності протоколів боротьби з відмиванням грошей та фінансуванням тероризму на мінливому ландшафті віртуальних активів.
- **Управління ризиками:** ознайомлення учасників із золотими стандартами щодо пом'якшення різних ризиків, пов'язаних із віртуальними активами.
- **Нагляд за активами:** Надати учаснику найкращі практики в мистецтві влучної конфіскації та управління віртуальними активами під час розслідування.

Етапи зарахування:
Потенційні учасники можуть:

- Переглянути майбутні графіки семінарів і забезпечити собі місця.
- Звернутися по потенційні пільги щодо оплати на основі

їх професійного спектру за допомогою спеціальної форми.
- Уважно ознайомитися з чіткими умовами навчання та узгодити їх.

Цільова аудиторія:
Семінари розроблені таким чином, щоб знайти відгук у різноманітної аудиторії, включаючи слідчих, правників, співробітників фінансового регулювання, піонерів технологій, журналістів тощо. Вони обслуговують як державний, так і приватний сектори, обслуговуючи тих, хто цікавиться віртуальними активами та відповідними фіскальними нормами.

Структура оплати: Приблизна вартість навчання коливається від 10 000 доларів США до 20 000 доларів США залежно від кількості учасників. Преференційне ціноутворення потенційно доступне для представників державного сектору, науковців, некомерційних організацій та працівників засобів масової інформації.Додаткову інформацію про програму навчання можна запросити, звернувшись до Навчального відділу віртуальних активів УНЗ ООН за електронною адресою: cryptocurrency@unodc.org

Додаткові можливості: Платформа електронного навчання УНЗ ООН знаходиться за наступним посиланням: https://www.unodc.org/elearning/en/courses/course-catalogue.html

Базельський інститут врядування

Базельський інститут врядування: це незалежна некомерційна організація, яка зосереджена на вдосконаленні управління та протидії фінансовим злочинам у всьому світі. Базується в Базелі, Швейцарія, також працює в різних африканських країнах, тісно співпрацюючи з Базельським університетом.

Семінар з криптовалют Базельського інституту: пропонує комплексний 4-денний віртуальний тренінг, зосереджений на основах криптовалют, фінансових злочинів та дотриманні вимог щодо боротьби з відмиванням грошей. Курс охоплює практичний сценарій відмивання грошей, який допомагає учасникам відстежувати трансакції в блокчейні на предмет незаконної діяльності.

Вимоги: Відкритий для професіоналів з усього спектру, від правоохоронних органів, фінансового сектору, бізнесу та навіть студентів. Контент адаптований на користь політиків, регуляторів, журналістів-розслідувачів і будь-кого, хто цікавиться віртуальними активами, блокчейном та боротьбою із фінансовими злочинами.

Переваги: Семінар Базельського інституту пропонує інформацію про:
- **Основи криптовалюти:** розуміння основи, виникнення та масштабів віртуальних активів, технології розподіленого реєстру тощо.
- **Механіка трансакцій:** розуміння того, як функціонує мережа Bitcoin, криптографія та управління трансакціями.
- **Блокчейн і майнінг:** вивчення того, як трансакції захищаються, зберігаються та перевіряються в блокчейні.
- **Аналітика блокчейну:** методи моніторингу трансакцій у режимі реального часу, боротьба з ухиленням злочинців від встановлення особи, та використання інструментів.
- **Спеціальна перевірка:** Адаптація програм боротьби з відмиванням коштів та фінансуванням тероризму до нових способів оплати.
- **Управління ризиками:** найкращі практики та джерела управління ризиками віртуальних активів.
- **Арешт активів:** процедури та нюанси конфіскації криптоактивів, управління гаманцем тощо.

Хто може долучитися: Курс розроблений спеціально для слідчих, юристів, фахівців з протидії відмиванню коштів та фінансуванню тероризму, членів підрозділів фінансової розвідки, практиків FinTech, журналістів тощо. Він розроблений для професіоналів як державного, так і приватного секторів, які хочуть отримати знання у світі віртуальних активів та фінансових злочинів.

Вартість: 750 швейцарських франків за особу зі зниженою ставкою 300 швейцарських франків для деяких слухачів, таких як працівники державного сектору, науковці, некомерційні організації та журналісти.

Детальніше: info@baselgovernance.org

Деталі курсу та посилання на реєстрацію на доступні дати можна знайти на сторінці Базельського інституту у соціальних мережах.

Фонд по боротьбі з фінансовою злочинністю

Фонд FinCrime Fighters – це фонд, що базується у Стокгольмі, який був створений експертами Цільової групи з цифрових активів Глобальної коаліції з боротьби з фінансовими злочинами. Мета інструменту полягала в отриманні швидких відповідей з довідковою підтримкою на питання, пов'язані з фінансами на основі блокчейну та Web 3.

Фонд надає безкоштовний пул токенів для генеративного ШІ-Асистента, доступного виключно державним і приватним установам, які борються з фінансовими злочинами. Команда постійно завантажує і вивчає новітні доповіді, у тому числі матеріалів ОБСЄ, які були оприлюднені у відкритому доступі. По тексту нормативно-правових актів можна здійснювати пошук за допомогою системи, схожої на Chat GPT, щоб допомогти практикуючим фахівцям бути в курсі змін у регулюванні на щоденній основі.

https://www.fincrimefighters.com/

Рекомендації для правоохоронних органів після повідомлення про злочин

Рекомендації для правоохоронних органів після повідомлення про злочин

- **Надайте негайну підтримку:** переконайтеся, що жертви невідкладно отримують вказівки щодо того, як захистити свої цифрові активи, що залишилися, і зменшити ризик подальших фінансових втрат. Це може включати вказівки щодо зміни паролів, безпечних гаманців або переведення активів на більш безпечну платформу.
- **Фінансове консультування:** надайте жертвам фінансові консультаційні послуги, які можуть їм допомогти зрозуміти свої втрати, потенційні податкові наслідки та стратегії відновлення або мінімізації втрати з часом.
- **Просвіта:** Запустіть інформаційно-просвітницькі кампанії та семінари з питань такого шахрайства. Чим більше поінформована громадськість, тим складніше стає шахраям обдурити потенційних інвесторів.
- **Співпрацюйте з біржами:** Тісно співпрацюйте з криптовалютними біржами для відстеження та, можливо, заморожування активів шахраїв, що ускладнює для них переведення в готівку своїх незаконно отриманих прибутків.
- **Транскордонна співпраця:** оскільки цифрове шахрайство часто перетинає кордони, співпрацюйте з міжнародними правоохоронними органами для відстеження, затримання та судового переслідування винних.

Маріам Грігалашвілі поділилася думками з Грузії та Національного банку Грузії з колегами з Центрального банку Вірменії в Єревані під час семінару, присвяченого оподаткуванню криптовалюти та її зв'язку з політиками протидії відмиванню коштів та фінансуванню тероризму.

Висновки та принципи співробітництва з ОБСЄ

Висновки та принципи співробітництва з ОБСЄ

Ініціатива ОБСЄ з підтримки віртуальних активів

Хто ми?

Група експертів з віртуальних активів ОБСЄ унікально пристосована до відповіді на нові виклики, пов'язані з віртуальними активами, для політиків і правоохоронних органів. Спираючись на майже п'ятдесят років передового досвіду в наданні технічної експертизи, ми допомагаємо політикам та представникам правоохоронних органів орієнтуватися у складнощах віртуальних активів в межах 57 держав-учасниць ОБСЄ.

Цінність, яку ми створюємо для правоохоронних органів і політиків

- **Передові знання:** Наш тренінг пропонує правоохоронним органам і політикам актуальні ідеї та стратегії, розроблені для вирішення унікальних проблем у сфері віртуальних активів.
- **Операційна ефективність:** Завдяки практичному навчанню ми забезпечуємо логістику, бронюємо майданчики, запрошуємо попередньо перевірених експертів з віртуальних активів з держав-учасниць ОБСЄ, пропонуємо порядок денний та формуємо цілі навчання.
- **Навчання та підвищення кваліфікації:** Ми пропонуємо комплексні навчальні програми з віртуальних активів. Наша команда, яка складається з політиків, правоохоронних органів, членів комплаєнс-команд традиційних банків та компаній WEB3, надає пріоритет практичному навчанню з обмеженою та лаконічною теоретичною складовою. Основна увага приділяється практичним вправам, що забезпечують застосовність у реальному світі. Примітно, що попередні учасники побачили прямі результати навчань, включаючи успішне розслідування складних справ про відмивання грошей.
- **Забезпечення ресурсами:** Ми співпрацюємо з провідними експертами з блокчейну. Цей практичний досвід роботи з професійними інструментами дозволяє учасникам ефективно впроваджувати свої знання на сесіях глибокого занурення та семінарах, на яких ми перетворюємо складні новітні питання на вправи.
- **Аналіз справ:** Наш тренінг часто включає в себе дослідження кейсів у режимі реального часу та підтримку законодавчої роботи, яка візуалізує поточні події для забезпечення того, що ми вирішуватимемо проблеми раніше, ніж вони насправді виникнуть.
- **Масштабованість і безперервність:** Наша система каскадного навчання включає модель «підготовки тренерів», в рамках якої ми надаємо експертам можливість повернутися до своєї юрисдикції для подальшого поширення цих знань. Це забезпечує більш широке охоплення та безперервність у розвитку експертизи в країнах походження.
- **Створення безпечнішого цифрового середовища:** забезпечуючи належний інструментарій політиків і правоохоронних органів для роботи з віртуальними активами, ми робимо значний внесоку створення більш безпечного та прозорого цифрового фінансового ландшафту.

Приєднуйтесь до нас у формуванні майбутнього кібербезпеки та забезпеченні безпечнішого та прозорішого цифрового простору для всіх.

Зв'яжіться з нами за адресою: VirtualAssets@osce.org

Коротка добірка додаткової літератури

Коротка добірка додаткової літератури

Управління Організації Об'єднаних Націй з наркотиків і злочинності (UNODC)

Базовий підручник з виявлення та розслідування відмивання доходів, отриманих злочинним шляхом, з використанням віртуальних валют (2014)

Незважаючи на те, що цей всеосяжний 200-сторінковий документ був опублікований УНЗ ООН більше десяти років тому, він глибоко занурюється в різні поняття і надає контекст для термінів, описаних у цьому огляді. Він також містить детальні анкети для самооцінки:

https://www.unodc.org/documents/middleeastandnorthafrica/money-laundering/FULL10-UNODCVirtualCurrencies-final.pdf.pdf

Організація з безпеки і співробітництва в Європі (ОБСЄ)

Посібник із поводження з віртуальними валютами у кримінальних провадженнях (2022)

https://www.osce.org/files/f/documents/2/0/522754.pdf

Міністерство юстиції США

Роль правоохоронних органів у виявленні, розслідуванні та переслідуванні злочинної діяльності, пов'язаної з цифровими активами (2022)

https://www.justice.gov/d9/2022-12/The%20Report%20of%20the%20Attorney%20General%20Pursuant%20to%20Section.pdf

Доповідь, опублікована Міністерством юстиції США, є доповненням до міжнародного Звіту правоохоронних органів про співпрацю у сфері правозастосування та оновлення Рамкової системи контролю за дотриманням законодавства про криптовалюту. Вона містить вичерпний огляд для подальшого використання.

Про автора

Цей огляд був підготовлений Міхалом Громеком, провідним експертом з віртуальних активів у проекті ОБСЄ, спрямованому на зниження ризиків відмивання грошей, пов'язаних з віртуальними активами та криптовалютами, що реалізується в Офісі Координатора економічної та екологічної діяльності ОБСЄ (OCEEA). Громек є колишнім директором з комплаєнсу стокгольмської компанії VASP Safello, що торгує на Nasdaq. Він очолює Робочу групу з цифрових активів у Глобальній коаліції по боротьбі з фінансовими злочинами, яка співпрацює з Європолом, Всесвітнім економічним форумом і Лондонською фондовою біржею Risk Solutions. Громек також є членом керівної команди Глобальної коаліції по боротьбі з фінансовими злочинами. Він продовжує проводити тренінги для урядів та правоохоронних органів, надаючи підтримку у розробці законодавства для запобігання викликам, що стоять перед державами-учасницями ОБСЄ. Він здобув свій досвід на колишніх посадах керівника FinTech та програмного директора відділу управлінської освіти Стокгольмської школи економіки. Він працював з Fintech та Virtual Assets Compliance більше десяти років. Його висновки були опубліковані на Forbes.com, а також у низці книг і журналів.

Подяки

Цей посібник було суттєво удосконалено завдяки огляду та внескам, зробленим доктором Олександрою Андхов. Її юридична експертиза та розуміння значно підвищили точність, актуальність та глибину представленого контенту. Маючи досвід роботи доцентом юридичного факультету Копенгагенського університету, вона надала безцінні оцінки та рекомендації для написання цього документа. Доктор Андхов має досвід роботи на перетині права та технологій, беручи участь у значній кількості проектів у цій сфері, зокрема, як співзасновник та головний юридичний директор організації Financial Crime Fighters.

Щоб забезпечити максимально можливу читабельність і якість, документ було відредаговано кількома особами, переважно Грейс Маршалл, що забезпечило зрозумілість і зв'язність протягом усієї публікації. Як генеральний секретар Глобальної коаліції з боротьби з фінансовими злочинами, вона допомогла адаптувати інформацію для широкої аудиторії.

Окрім пані Маршалл, Деніссе Рудіч надала тривалу підтримку в оцінці та редагуванні документа, застосувавши свій великий досвід роботи у цій сфері. Її розуміння як змісту, так і мови було незамінним.

Подальшу редакційну підтримку надали Грета Баркаускієне, Емілія Пахомов, Сонгьонг Кан та Вінсент Данжан. Додатковий огляд та пропозиції щодо внесення змін були проведені Центром Інтерполу з питань боротьби з фінансовими злочинами та корупцією (IFCACC), зокрема Моною Гессейн, а також членами Європейського центру кіберзлочинності (EC3), зокрема Гертом Яном ван Хардевельдом.

Колектив Офісу Координатора з питань економічної та природоохоронної діяльності ОБСЄ вдячний за таку потужну підтримку.

Ми щиро вдячні Латвійському підрозділу фінансової розвідки за їх важливу роль у виявленні та відборі лідерів екосистем для навчального візиту до країн Балтії, присвяченого віртуальним активам. Ми також висловлюємо вдячність Міністерству фінансів Польщі за його постійну підтримку у наданні навчальних приміщень. Крім того, ми глибоко вдячні багатьом установам та особам з широкого кола секторів, чий внесок відіграв важливу роль в успішному просуванні проекту.

Нотатки

ОБСЄ Організація з безпеки та співробітництва в Європі

Секретаріат ОБСЄ
Офіс Координатора економічної та природоохоронної діяльності ОБСЄ
Відділ економічного врядування
Вальнерштрассе 6
1010 Відень, Австрія
E-mail: virtualassets@osce.org
www.osce.org/eea