Înțelegerea infracționalității cripto

Ghid pentru organele de aplicare a legii

OSCE Organization for Security and Co-operation in Europe

Declinare de responsabilitate

Această publicație a fost pregătită în baza materialului original oferit de autor. Conținutul de față nu a fost supus editării de către redacția OSCE. Opiniile exprimate aici reprezintă responsabilitatea autorului și nu reflectă neapărat punctele de vedere ale OSCE, ale misiunilor sau ale statelor sale participante.

OSCE, misiunile sale și statele sale participante își declină orice responsabilitate pentru orice consecințe care ar putea rezulta din utilizarea acestei publicații. Această publicație nu abordează chestiuni legate de responsabilitatea legală sau de oricare altă natură pentru acțiuni sau omisiuni din partea oricărei persoane. Menționarea sau referirea la anumite țări sau teritorii în această publicație nu implică nicio poziție a OSCE cu privire la statutul lor juridic, autoritățile de guvernare, instituțiile sau delimitarea granițelor acestora.

Înțelegerea infracționalității cripto

Ghid pentru organele de aplicare a legii

Organization for Security and Co-operation in Europe

Cuprins

Acronime, abrevieri și termeni cheie cu explicații

A 5-a directivă CSB	Directiva (UE) 2018/843 a Parlamentului European și a Consiliului din 30 mai 2018 cu privire la modificarea Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, și modificarea Directivelor 2009/138/CE și 2013/36/UE (Text cu relevanță pentru SEE). Această directivă a fost extinsă prin adăugarea criptoactivelor în domeniul său de aplicare. Până la 10 ianuarie 2020, statele membre trebuie să pună în aplicare legile și regulamentele necesare pentru a implementa prezenta directivă.
CSB	Combaterea spălării banilor se referă la legile, reglementările și procedurile menite să împiedice infractorii să mascheze fondurile obținute ilegal ca venituri legitime.
CASP	Furnizori de servicii de criptoactive – entități care furnizează publicului servicii de criptoactive. Aceste servicii pot cuprinde o gamă largă de activități, inclusiv, dar fără a se limita la: 1. Servicii de schimb: facilitarea cumpărării și vânzării de criptoactive pentru bani FIAT sau alte criptoactive. 2. Furnizori de portofele cripto: oferă portofele cu sau fără custodie pentru a stoca, gestiona și transfera criptoactive. 3. Servicii de transfer: permite transferul de criptoactive de la o adresă la alta sau de la un cont la altul. 4. Consultanță financiară: oferirea de consultanță cu privire la cumpărarea, vânzarea sau deținerea de criptoactive. 5. Servicii de custodie: deținerea și protejarea criptoactivelor în numele clienților. (Vedeți p. 20 pentru mai multe informații.)
CoE	Consiliul Europei – organizație internațională dedicată apărării drepturilor omului, democrației și statului de drept în Europa.
CFT	Combaterea Finanțării Terorismului – se referă la politici și acțiuni de prevenire a finanțării activităților teroriste. Această instituție urmărește să detecteze și să oprească fluxul de bani, atât din surse legitime, cât și din cele ilicite, către grupuri care intenționează să comită acte de terorism.
Jetoane ERC20	Jetoanele Ethereum Request for Comments 20 – implementat în 2015, este un standard tehnic utilizat pentru crearea și emiterea de contracte inteligente pe blockchain-ul Ethereum.
UE	Uniunea Europeană – organizație politică și economică din care fac parte 27 de țări din Europa.
EPE	Platforma Europol pentru experți – un spațiu condus de Europol pentru experții în aplicarea legii, destinat schimbului de cunoștințe, bune practici și date fără caracter personal despre criminalitate.
EUROPOL	Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii – Agenția Uniunii Europene de aplicare a legii care asistă statele sale membre în lupta lor împotriva infracțiunilor internaționale grave și a terorismului.
GAFI	Grupul de Acțiune Financiară – un organism interguvernamental de stabilire a standardelor, fondat pentru a dezvolta politici de combatere a spălării banilor și finanțării terorismului.

FinCEN	Rețeaua de Combatere a Infracțiunilor Financiare este un birou al Departamentului Trezoreriei Statelor Unite ale Americii care colectează și analizează informații despre tranzacțiile financiare.
UIF	Unitate de informații financiare – o agenție guvernamentală responsabilă pentru colectarea, analiza și diseminarea informațiilor financiare și a informațiilor privind activitățile suspecte de spălare a banilor și finanțare a terorismului.
IP	Internet Protocol – un set de reguli care guvernează modul în care datele sunt transmise prin internet sau alte rețele.
LER	Interpelare din partea organelor de aplicare a legii – O cerere făcută de agențiile de aplicare a legii către companii sau persoane fizice, prin care se solicită informații pentru investigații.
MiCA	Regulamentul (UE) 2023/1114 al Parlamentului European și al Consiliului, din 31 mai 2023, privind piețele criptoactivelor și de modificare a Regulamentelor (UE) nr. 1093/2010 și (UE) nr. 1095/2010 și a Directivelor 2013/36/UE și (UE) 2019/1937. Este un nou regulament UE care reglementează activele cripto și care a intrat în vigoare la 30 decembrie 2024.
SB	Spălare de bani – procesul ilegal prin care sume mari de bani, obținute dintr-o activitate infracțională, sunt făcute să pară că provin din surse legitime.
Portofel MultiSig	Portofel de criptomonede cu semnături multiple – tip de portofel de criptomonede care necesită mai multe chei private pentru a autoriza o tranzacție.
OCEEA	Biroul Coordonatorului Activităților Economice și de Mediu al OSCE
OSCE	Organizația pentru Securitate și Cooperare în Europa – O organizație regională de securitate în Europa, axată pe promovarea dialogului și cooperării între dimensiunile militare, politice, de mediu și economice.
OSINT	Open source intelligence (informații din surse deschise) – informații colectate din surse disponibile public, utilizate într-un context de investigație.
OTC	Over the counter (direct la ghișeu) – tranzacționarea de active virtuale între două părți cu sau fără implicarea unei platforme centralizate de schimb sau a unui broker.
UNODC	Oficiul Națiunilor Unite pentru Droguri și Criminalitate este un organism în cadrul Organizației Națiunilor Unite responsabil de producerea și diseminarea datelor despre droguri și criminalitate.
VASP	Furnizor de servicii de active virtuale – un termen introdus de GAFI pentru a desemna o entitate care desfășoară activități sau operațiuni cu active virtuale. (Pentru mai multe informații vedeți p. 20)
VPN	Rețea privată virtuală – o tehnologie care permite crearea unei conexiuni securizate peste o rețea mai puțin sigură între computerul unei persoane și internet, uneori, dar nu întotdeauna, pentru a ascunde locația utilizatorului.

Introducere

Scopul acestui ghid

Acest document servește drept ghid cuprinzător pentru ofițerii de aplicare a legii, inclusiv pentru polițiști, procurori, agenți de stat și federali, precum și pentru specialiști în domeniul fiscal și criminaliști care au fost recent introduși în domeniul criptomonedelor și a altor active virtuale. Este gândit pentru cei care sunt din ce în ce mai implicați în investigarea infracțiunilor cripto.

Ghidul se concentrează pe cele mai obișnuite tipuri de înșelătorii și comportamente frauduloase, explică cele mai bune practici pentru ofițeri, ce acțiuni să întreprindă și ce tip de informații pot fi consemnate de la potențialele victime, în special în cadrul procesului inițial de colectare a probelor la secțiile locale de poliție.

Acest ghid a fost scris și conceput pentru a îndruma ofițerii de aplicare a legii și nu acoperă, în mod intenționat, domenii ale criptomonedelor ce nu sunt foarte relevante în cazurile investigate de poliție care au legătură cu victime individuale. De asemenea, ghidul de față se concentrează în mod intenționat pe interacțiunile dintre autoritățile de aplicare a legii și persoanele fizice. Informațiile despre STR-uri (Raportări de tranzacții suspecte) sau SAR-uri (Raportări de activități suspecte) utilizate de instituțiile financiare sau de agențiile de informații financiare (sau echivalentele acestora) nu au fost luate în considerație.

În modul în care au fost tratate cazurile care implică criptomonede până în prezent au fost identificate multiple probleme. De exemplu, din cauza colectării incomplete a datelor, anchetatorii au raportat că au trebuit să ia legătura cu victimele pentru a colecta informații precum adresa unui portofel de criptomonede, fără de care o investigație rămâne imposibilă.

Ofițerii au nevoie să înțeleagă ce informații sunt esențiale pentru a fi colectate. O asemenea comunicare defectuoasă adesea cauzează întârzieri de mai multe zile, deoarece este posibil ca victimele să nu înțeleagă pe deplin ce informații sunt relevante pentru aplicarea legii.

Această lipsă de cunoștințe nu este doar un inconvenient, ci este exploatată de infractorii care au conștientizat că, deși tehnologia este disponibilă la nivel global încă de când apare, practicile în investigarea criptomonedelor continuă să rămână în urmă. Ca răspuns la această provocare din ce în ce mai mare, am elaborat acest ghid care descrie modul în care organele de aplicare a legii ar trebui să procedeze în investigarea și în asistarea potențialelor victime care raportează săvârșirea unei infracțiuni legate de criptomonede.

Recunoscând complexitatea subiectului și diversitatea situațiilor și practicilor legale din diferitele state participante la OSCE, scopul nostru nu este de a oferi un ghid detaliat, ci mai degrabă un manual practic care poate fi utilizat ad-hoc de către agenții de aplicare a legii din prima linie care primesc sesizări de la cetățeni.

Ghidul de față are ca scop generarea de conversații despre cum pot fi îmbunătățite bunele practici interne, în special în cazurile în care liniile directoare existente nu acoperă criptomonedele. Cele mai frecvente practici frauduloase au fost rezumate așa cum se desfășoară în prezent, iar acest material introductiv este oferit pentru a facilita o înțelegere mai aprofundată asupra subiectului.

Acest ghid servește ca o piatră de temelie în reducerea decalajului dintre aplicarea legii și contextul în continuă schimbare al activelor virtuale. Trebuie recunoscut faptul că spațiul Web3 în care operează criptomonedele evoluează rapid și că s-ar putea impune ca acest ghid să fie completat cu cunoștințe suplimentare.

Acest ghid pune în evidență nu numai instrumentele și strategiile necesare pentru conducerea unor investigații eficiente, ci își propune, de asemenea, să încurajeze colaborarea și învățarea continuă în cadrul comunității. Scopul final este de a dota ofițerii de aplicare a legii cu cunoștințele și încrederea necesare pentru a face față provocărilor unice reprezentate de infracțiunile legate de criptomonede.

Structura ghidului

Scopul principal al acestui ghid este de a educa ofițerii de aplicare a legii pentru care domeniul infracțiunilor cu active virtuale este o noutate și de a sprijini victimele care raportează astfel de infracțiuni. Având în vedere acest obiectiv, ghidul este structurat după cum urmează:

În primul rând, sunt oferite informații concise privind activele digitale. Activele digitale pot fi înțelese ca un termen general care include subiecte precum criptomonedele, cum ar fi Bitcoin și Ethereum. Se oferă o explicație despre ce sunt acestea și cum sunt asemănătoare sau diferite una de cealaltă.
Sunt examinate diferențele și asemănările dintre ele pentru a asigura o înțelegere clară. Mai mult decât atât, sunt menționate potențiale utilizări și abuzuri de criptomonede și tehnologia care stă la baza acestora.

După stabilirea unei înțelegeri fundamentale a activelor virtuale, ghidul prezintă infracțiunile frecvente asociate cu acestea. În continuare, manualul descrie protocoalele standard pentru gestionarea acestor infracțiuni, identificându-le pe cele care pot fi soluționate rapid și pe cele care necesită investigații mai amănunțite. Ghidul include, de asemenea, colectarea de probe pentru fiecare infracțiune, întrebări ce pot fi adresate victimelor, date ce pot fi partajate cu furnizorii de servicii de active virtuale și informații care pot fi obținute din schimburile de active virtuale.

Accesibilitatea și simplificarea limbajului: dată fiind complexitatea domeniului, autorii au folosit un limbaj simplificat și non-tehnic pentru a face acest material accesibil începătorilor. Evitându-se jargonul, scopul este să se asigure claritatea conținutului, pentru ca acesta să fie ușor de înțeles de către toți cititorii. În cele din urmă, ghidul oferă surse de sprijin pentru victime și prezintă diverse sugestii care pot ajuta la prevenirea infracțiunilor legate de criptomonede.

Context

Investigațiile centrate pe activele cripto ar putea părea intimidante la început, mai ales date fiind concepțiile greșite referitoare la dificultatea recuperării activelor. Este un mit faptul că, odată ce o monedă națională a fost convertită într-o criptomonedă precum Bitcoin, fondurile sunt pierdute iremediabil, victimele nu mai pot face nimic iar anchetatorii sunt nevoiți să-și închidă cazurile. Această percepție a fost corectă până acum câțiva ani, însă vremurile s-au schimbat.

Progresul tehnologic a deschis noi uși, similar cu modul în care verificarea ADN a permis redeschiderea și rezolvarea cazurilor vechi, rămase nesoluționate. Acum putem redeschide dosarele de criptomonede clasate anterior. Accesibilitatea tot mai mare a instrumentelor concepute pentru detectarea și verificarea tranzacțiilor cu criptomonede în blockchain și modificările în dreptul internațional ne permit să identificăm autorii infracțiunilor cu criptomonede. Aceste instrumente devin tot mai ușor de utilizat și tot mai larg răspândite, anunțând o schimbare în peisajul investigațiilor.

În ciuda tuturor acestor instrumente, vedem încă multe investigații efectuate de ofițerii de poliție locali care sunt clasate prematur din cauza înțelegerii și a cunoștințelor limitate. În contrast cu opinia general acceptată, tranzacțiile cu criptomonede pot fi urmărite. Dacă datele sunt introduse corect de la început, există o mare probabilitate ca tranzacțiile să poată fi legate de un potențial suspect, iar probele virtuale și fizice să fie corelate fără dificultate.

În ultimii ani, mai multe state participante la OSCE au început să integreze criptomonedele și alte active virtuale în reglementările naționale de combatere a spălării banilor, în conformitate cu standarde actualizate emise de Grupul de Acțiune Financiară (GAFI). Această evoluție implică faptul că entitățile care operează cu criptomonede trebuie acum să adere la procesele concepute inițial pentru instituțiile bancare tradiționale. Acestor entități li se cere să verifice identitatea clienților lor, să cerceteze sursele de fonduri și să monitorizeze unde sunt trimise criptomonedele.

În virtutea acestor schimbări, Echipa Experților OSCE în domeniul Activelor Virtuale (OSCE Virtual Asset Expert team) a decis să lanseze un ghid special adaptat membrilor unităților locale de aplicare a legii. Acest ghid nu doar va evidenția noile posibilități în investigarea criptomonedelor, ci va oferi, de asemenea, ofițerilor de aplicare a legii cunoștințele și instrumentele necesare pentru a urmări dreptatea în acest domeniu complex și în continuă evoluție.


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
(PCPM)

Despre OSCE

OSCE este Organizația pentru Securitate și Cooperare în Europa. Aceasta funcționează ca o organizație regională de securitate care are scopul de a promova dialogul și cooperarea, adoptând o viziune cuprinzătoare asupra securității, de la dimensiunile militare și politice la cele de mediu și economice.

OSCE a fost înființată în timpul Războiului Rece în 1975 și este formată în prezent din 57 de state participante. Aceste state sunt predominant din Europa, unde se concentrează o mare parte din activitatea OSCE, dar includ și țări din America de Nord, precum Canada și Statele Unite, și din Asia Centrală, cum ar fi Kazahstan, Kârgâzstan și Uzbekistan. OSCE funcționează pe principiile securității cuprinzătoare, care include dimensiunile militare, politice, economice, de mediu și umane.

În Europa, misiunea OSCE este de a încuraja stabilitatea și a gestiona provocările de securitate. Scopul său principal este acela de a preveni conflictele și de a promova cooperarea regională prin mecanisme precum negocierile diplomatice, inițiativele de soluționare a conflictelor și acordurile de control asupra armelor. Mai mult decât atât, OSCE depune eforturi pentru a sprijini democrația și drepturile omului, cum ar fi prin monitorizarea alegerilor.

În ceea ce privește infracțiunile financiare și criminalitatea cripto, OSCE contribuie la combaterea acestor provocări prin facilitarea schimbului de informații și prin dezvoltarea de capacități între statele sale participante, îmbunătățind astfel fluxul de informații transfrontaliere. Aceasta este o activitate importantă, deoarece infracțiunile cripto, prin natura lor, nu se limitează la o singură țară sau monedă și, prin urmare, cooperarea între state este vitală.

OSCE încurajează, de asemenea, instituirea unor cadre juridice și a unor măsuri de reglementare solide, atât pentru a combate spălarea banilor și finanțarea terorismului în forma lor clasică, cât și pentru a detecta și preveni activitățile ilicite care implică criptomonede. Acest fapt presupune asigurarea că statele participante respectă standardele internaționale de combatere a spălării banilor și a finanțării terorismului.

În acest sens, OSCE organizează programe de formare și ateliere de lucru cu intenția de a îmbunătăți cunoștințele agenților de aplicare a legii, instituțiilor financiare și ale altor actori relevanți în combaterea infracțiunilor financiare și cripto. Aceste eforturi au ca scop îmbunătățirea tehnicilor de investigație și utilizarea tehnologiilor de ultimă oră pentru detectarea și combaterea criminalității cibernetice și a activităților infracționale legate de criptomonede.

Prin prezenta publicație, OSCE răspunde nevoii anumitor state participante de a atenua riscurile generate de utilizarea activelor virtuale în scopuri ilicite și pentru eludarea sancțiunilor internaționale. Reducerea riscurilor este, așadar, obiectivul principal al proiectului „Soluții inovatoare de politici pentru atenuarea riscurilor de spălare a banilor aferente activelor virtuale” condus de Biroul Coordonatorului Activităților Economice și de Mediu al OSCE (OCEEA).

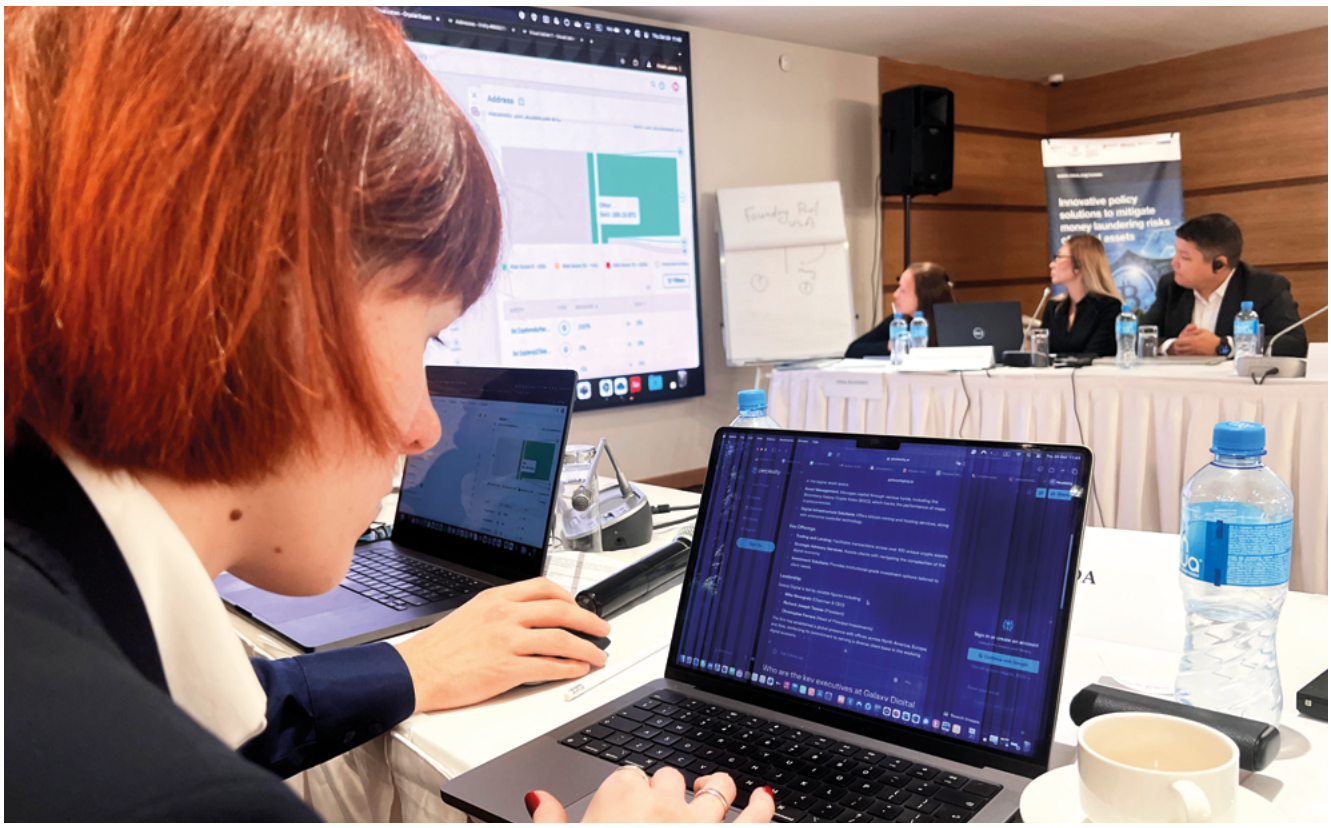
Obiectivul final al acestui proiect este de a consolida capacitățile autorităților naționale pentru a contracara vulnerabilitățile specifice activelor virtuale.

Pe parcursul implementării proiectului, OCEEA, împreună cu Programul Global pentru Combaterea Spălării Banilor al Oficiului Națiunilor Unite pentru Droguri și Criminalitate (UNODC GPML), au continuat să asiste trei țări din Europa de Est și Caucaz (Georgia, Republica Moldova și Ucraina) în vederea armonizării cadrului lor de reglementare pentru activele virtuale (VA) și furnizorii de servicii privind activele virtuale (VASP) cu recomandările GAFI, oferind totodată organelor relevante de aplicare a legii din aceste trei țări sprijin tehnic și facilitând consolidarea capacităților.

Pentru a spori eficiența proiectului, echipa OSCE a încheiat un parteneriat cu UNODC, care a contribuit la rândul său cu propria expertiză și cu programe de formare practică pe teme precum criptomonedele, riscurile de spălare a banilor și finanțare a terorismului, investigarea, sechestrarea și confiscarea, reglementarea și evaluarea riguroasă a clienților (*customer due diligence*). OCEEA continuă să sprijine autoritățile relevante precum băncile centrale, departamentele de conformitate ale instituțiilor financiare cheie, unitățile de informații financiare, procuraturile generale, ministerele de justiție și de afaceri interne, prin oferirea de asistență pentru elaborarea de reglementări și instrucțiuni pentru personal, organizarea de activități de conștientizare și informare și facilitarea cooperării interinstituționale și internaționale în investigarea infracțiunilor comise cu utilizarea criptomonedelor.

Această publicație a fost creată ca parte a soluțiilor inovatoare de politici de atenuare a riscurilor de spălare a banilor ale proiectelor de active virtuale, finanțate de Germania, Italia, Polonia, România, Regatul Unit și Statele Unite.

OSCE Organization for Security and Co-operation in Europe



Greta Barkauskienė conduce un atelier pentru anchetatori în Astana, Kazahstan. Bazându-se pe experiența sa vastă ca expert în CSB (Combaterea Spălării Banilor) și în calitate de coordonator al Grupului național de cooperare tactică de pe lângă Centrul de Excelență în Combaterea Spălării Banilor din Lituania, fondat ca parteneriat public-privat, ea transmite cele mai bune practici însușite atât de la actorii publici, cât și de la cei privați, pentru a capacita țările beneficiare.

Atelierele pentru anchetatori organizate în Tbilisi, Georgia, s-au concentrat pe aspectele cheie privind sechestrarea activelor de tip criptomonede, inclusiv pe pregătirea unor condiții securizate pentru potențiale confiscări. Aceste ateliere au fost urmate de un exercițiu de îmbunătățire a abilităților de identificare, transfer și recuperare a activelor de tip criptomonede din Blockchain. Foto: Michal Gromek.

Înțelegerea activelor digitale: Un ghid simplificat

Înțelegerea activelor digitale: un ghid simplificat

În această secțiune vom explica diferențele dintre diverse active digitale, FIAT și criptomonede. De asemenea, vom evidenția diferențele dintre diferitele tipuri de criptomonede și infrastructura din jurul lor.

Există adesea o confuzie cu privire la diferențele dintre activele digitale, activele virtuale, activele cripto și criptomonedele.

Mai simplu spus, **activul digital** este termenul cel mai larg ce se referă la un activ care există în formă digitală. Acesta include imagini, videoclipuri, muzică, de exemplu în format MP3, documente și monede virtuale.

Activul virtual este un set mai restrâns de active digitale. Conform GAFI,[1] activele virtuale (criptoactivele) se referă la orice reprezentare digitală a valorii care poate fi tranzacționată, transferată sau utilizată digital ca mijloc de plată. Aceasta nu se referă la reprezentarea digitală a monedelor FIAT.

Spre deosebire, **activul cripto** (sau criptoactivul) ocupă o nișă și mai îngustă. Este un activ care stochează valoare, dar trebuie transferat prin tehnologia registrelor distribuite (DLT). Blockchain este un tip de DLT. Puteți avea un activ virtual precum o monedă într-un joc online care nu este un activ cripto, deoarece este transferat între jucători în cadrul jocului fără a se utiliza tehnologia registrului distribuit. Blockchain este în prezent cel mai proeminent tip de tehnologie de registru distribuit, dar există și alte tehnologii DLT, cum ar fi Hashgraph, Iota Tangle, R3 Corda și multe altele. Având în vedere scopul acestui ghid, ne vom concentra pe finanțele bazate pe blockchain.

Domeniul activelor digitale cuprinde mai multe active de diferite tipuri, cum ar fi criptomonedele, ce reprezintă noi tipuri de monedă care funcționează folosind tehnologia blockchain, și jetoanele nefungibile (NFT), care sunt active bazate pe imagini.

Astfel, odată ce un activ cripto este elaborat pentru a fi tranzacționat, transferat sau utilizat ca mijloc de plată, îl numim criptomonedă. Mai este răspândit și termenul de valută sau monedă virtuală, utilizat adesea ca sinonim pentru criptomonedă. Factorul distinctiv dintre criptomonedă și valuta virtuală este tehnologia subiacentă (sau tehnologia de bază). Criptomonedele folosesc blockchain, în timp ce monedele virtuale nu sunt neapărat construite pe tehnologia blockchain.

Acest ghid se va concentra predominant pe infracțiunile comise cu criptomonede.

Cu permisiunea autorului (citat din Alexandra Andhov, Computational Law, Karnov, 2022)

1 Grupul de Acțiune Financiară, sursa: https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,digital%20representation%20of%20fiat%20currencies (accesat: 26 sept. 2023).

Criptomonede vs. FIAT

Monedele tradiționale și banii de hârtie, cunoscuți sub numele de „monedă FIAT", au fost coloana vertebrală a economiilor noastre de secole. Însă, odată cu dezvoltarea tehnologiei, au apărut noi forme de bani, estompând granițele dintre tangibil și virtual. Când persoanele fizice efectuează transferuri electronice în monedă FIAT de la o persoană la alta, folosesc „e-money", sau bani electronici. E-money, sau banii electronici, reprezintă moneda noastră FIAT familiară într-o formă digitală, facilitând tranzacțiile electronice fără a modifica valoarea acesteia. Banii electronici sunt o reprezentare digitală a monedei fiat.

Spre deosebire de FIAT, criptomonedele operează într-un mediu descentralizat. Acestea nu se subsumă niciunui guvern sau bănci centrale, valoarea lor fiind determinată de diverși factori, inclusiv cererea, tehnologia și încrederea. Bitcoin, un nume de frunte în acest domeniu, a manifestat potențialul acestor valute, valoarea sa crescând la cote remarcabile. În 2021, a atins o valoare de peste 64 000 USD per monedă. Criptomonedele, cum ar fi Bitcoin și Tether, nu sunt garantate de niciun guvern sau bancă centrală. Deși nu sunt nici pe departe la fel de vechi ca valuta FIAT, monedele virtuale nu sunt atât de noi pe cât presupun majoritatea oamenilor. Una dintre primele monede virtuale – E-Gold – a fost introdusă în urmă cu aproape 30 de ani, în 1996.

Sumar despre E-Gold

Una dintre primele monede virtuale populare s-a numit „E-Gold". Înființată pentru prima dată în 1996 de Douglas Jackson și Barry Downey, E-Gold a permis utilizatorilor să deschidă un cont cu o valoare denominată în grame de aur (sau alte metale prețioase), oferindu-le posibilitatea de a efectua transferuri instantanee de valoare către alte conturi E-Gold.

În 2005, E-Gold avea 2,5 milioane de titulari de cont ce efectuau tranzacții zilnice la o valoare tipică de 6,3 milioane USD. Această monedă a fost populară datorită eficienței, comisioanelor mici și accesibilității globale. Cu toate acestea, în lipsa reglementărilor stricte, acest instrument a devenit atractiv și pentru activități ilicite. În 2007, un juriu din Statele Unite a pus sub acuzare compania E-Gold pentru spălare de bani, conspirație și administrare fără licență a unei afaceri de transmitere de bani, ceea ce a dus în cele din urmă la închiderea E-Gold de către instanțele din SUA în 2009. E-Gold a inspirat numeroși imitatori, precum e-Bullion.com, Pecunix.com și alții.[2]

Este important să fim specifici atunci când vorbim despre acest domeniu, deoarece monedele virtuale se pot referi atât la moneda electronică/banii electronici, cât și la criptomonede. Lucrul acesta poate deveni rapid derutant. În ghidul de față, ne vom concentra pe criptomoned

Tehnologie de bază: Blockchain

Blockchain este o tehnologie de registru distribuit (DLT). Această tehnologie nouă a apărut pentru prima dată în 2008 într-un document tehnic publicat de Satoshi Nakomoto.[3] Este definită ca fiind descentralizată, deoarece nu există un singur centru de control sau o singură persoană responsabilă. Orice utilizator poate face modificări, însă, pentru a deveni permanente, ele trebuie acceptate de către majoritatea utilizatorilor.

Există o mare varietate de blockchain-uri. În termeni simpli, blockchain se referă la tehnologia de bază. Imaginați-vă că fiecare blockchain este o clădire. În timp ce la exterior toate clădirile pot arăta foarte diferit și pot avea utilizări diferite, atunci când ne uităm dedesubt, aproape toate sunt construite din cărămizi și

2 "Feds accuse E-Gold of helping cybercrooks", NBC News, May 2007./ „Federalii acuză E-Gold că a ajutat infractorii cibernetici", NBC News, mai 2007. (Disponibil la: http://redtape.nbcnews.com/news/2007/05/02/6346006-feds-accuse-e-gold-of-helpingcybercrooks (accesat: 24 august 2023).

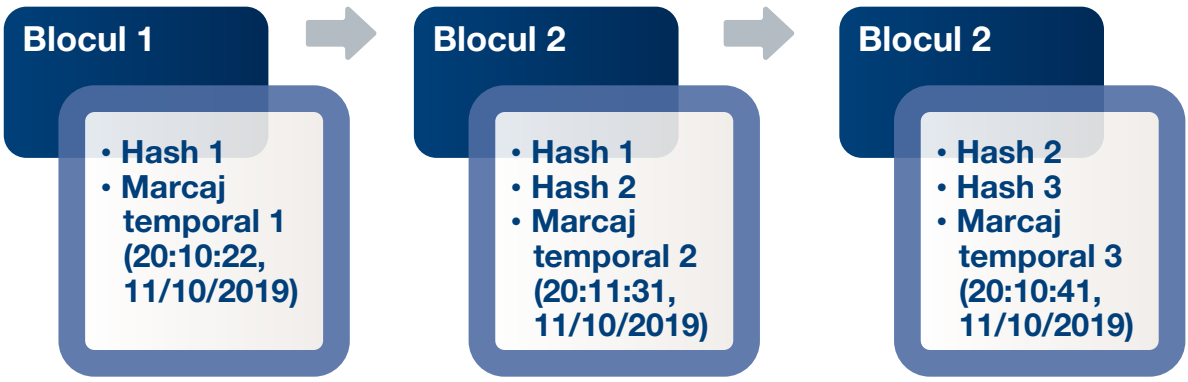
"Internet currency firm pleads guilty to money laundering", The Industry Standard, July 2008./ „O companie de monede pe internet se declară vinovată de spălare de bani", The Industry Standard, iulie 2008. Disponibil la: http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering (accesat: 24 august 2023). *Synopsis of e-gold Transactions (1996) E-Gold./ Pe scurt despre tranzacțiile e-gold (1996) E-Gold.* Disponibil la: http://www.e-gold.com/unsecure/synopsis.htm (accesat: 24 aug. 2023).

3 Nakamoto, S. (2008) "A peer-to-peer electronic cash system", Bitcoin./ Nakamoto, S. (2008) „Un sistem electronic de numerar de la egal la egal", Bitcoin. Disponibil la: https://bitcoin.org/en/bitcoin-paper (accesat: 26 august 2023).

ciment.
La fel ca în cazul clădirilor, unele blockchain-uri pot fi accesate de oricine fără a avea nevoie de permisiune, în timp ce altele necesită aprobare înainte de a vi se permite să vă alăturați. În acest sens, este important să facem distincția dintre blockchain-urile publice și cele private. Blockchain-urile publice sunt cele „fără permisiune" necesară și tind să solicite mai puțină transparență sau control, în timp ce blockchain-urile „cu permisiune" sunt adesea utilizate în scopuri de afaceri și impun ca persoana care dorește să se alăture să fie aprobată.

Blockchain-ul este numit astfel deoarece utilizatorii adaugă sau modifică „blocuri" de date, iar aceste blocuri sunt legate între ele într-un lanț cronologic (în funcție de timp). Când un utilizator face sau încarcă un nou bloc (de ex., o nouă tranzacție cu un bitcoin), toți ceilalți utilizatori de pe blockchain trebuie să valideze noul bloc folosind „metode de consens" (acest proces implică ecuații matematice destul de complexe și menit să asigure că blocul respectiv este de încredere). Deoarece blocurile sunt toate legate între ele, este aproape imposibil să mergi la un bloc anterior și să-l schimbi. Aceasta înseamnă că sistemul nu poate fi manipulat. Orice informație nouă (inclusiv modificarea unei informații vechi) este înregistrată într-un bloc nou.

Blockchain funcționează în așa fel încât permite tuturor utilizatorilor conectați la acel lanț să vadă întregul istoric al lanțului (așa numitul "ledger", sau „registrul"). Prin urmare, utilizatorii unui blockchain cu bitcoini pot vedea fiecare tranzacție care a fost făcută. Acest lucru permite anchetatorilor să efectueze investigații. Datorită distribuției registrului blockchain către fiecare utilizator, blockchain se mai numește și „tehnologia registrelor distribuite" sau DLT. Este ca o „foaie de calcul google" ("google sheet") în care toată lumea poate colabora și vedea versiunile anterioare. Totul este vizibil și nimic nu poate fi modificat fără ca toată lumea să vadă, iar aceasta caracteristică asigură un nivel ridicat de transparență, încredere și securitate. De asemenea, este astfel asigurat și un nivel ridicat de rezistență la atacuri: deoarece fiecare persoană are o copie de blockchain și nu există o versiune centralizată, chiar dacă un utilizator („nod" în terminologia blockchain) este atacat și eșuează, sistemul poate funcționa în continuare.



Cu permisiunea autorului (citat din Alexandra Andhov, Computational Law, Karnov, 2022).

Tipuri de criptomonede

Există două moduri de a face distincția între criptomonede:

- **Dacă sunt convertibile sau neconvertibile**
- **Dacă sunt centralizate sau descentralizate**

Aceste caracteristici distinctive sunt descrise mai detaliat mai jos.

Monede convertibile și neconvertibile

Monedele convertibile au o valoare echivalentă în moneda FIAT și pot fi schimbate înapoi în bani „normali". Convertibilitatea acestora nu este garantată, deoarece criptomonedele nu sunt susținute de niciun guvern sau instituție. Convertibilitatea unei criptomonede într-o monedă FIAT se bazează pe acceptarea ofertelor de piață și a celor private. Acesta este tipul de criptomonedă cu care se produc majoritatea infracțiunilor. Exemple de monede convertibile includ Bitcoin și E-Gold.

Monedele neconvertibile sunt ca monedele de aur care rămân în cadrul unui joc pe calculator. Infracțiunile comise cu acestea sunt mai puțin frecvente, deoarece ele nu au valoare reală. Cu toate acestea, unii indivizi găsesc o modalitate de a le tranzacționa în afara limitelor jocului în care există, făcându-le convertibile în afara jocului, chiar dacă acest lucru este împotriva regulilor

acelui joc. De exemplu, cineva poate transfera „monede de aur colectate” de la un jucător unui alt jucător într-un joc, tranzacția fiind achitată în numerar în lumea reală.

Monede centralizate și descentralizate

Criptomonedele centralizate sunt supravegheate de o singură autoritate care emite moneda, îi stabilește regulile, menține un registru de plăți și are competența de a o retrage din circulație. Monedele centralizate pot fi convertibile sau neconvertibile. Monedele neconvertibile sunt întotdeauna centralizate (deoarece, de exemplu, cineva nu poate avea o monedă într-un joc fără ca jocul respectiv să fie responsabil de acea monedă). Atunci când este schimbată o monedă convertibilă centralizată, rata de schimb este determinată de cererea și oferta pieței sau este fixată de administrator. Un bun exemplu de monedă centralizată este E-Gold.

Monedele descentralizate, pe de altă parte, nu se subsumă unei autorități centrale și funcționează în baza unei rețele de la egal la egal (peer-to-peer). Gândiți-vă la un sistem descentralizat precum internetul. Așa cum nu există un singur supraveghetor responsabil de întreg internetul, un sistem descentralizat nu are o autoritate principală de control. Chiar dacă majoritatea oamenilor folosesc internetul zilnic, nu există o singură entitate care să fie plătită; în schimb, diferiți furnizori sunt plătiți pentru diferite servicii. Acesta este modul în care este utilizată tehnologia de rețea blockchain din spatele criptomonedelor precum Bitcoin. Tranzacțiile sunt gestionate prin rețea și nu există nicio altă formă de monitorizare din partea niciunei autorități.

Mai jos găsiți o selecție de zece criptomonede cu cele mai mari capitalizări de piață (la data de 23 august 2023), în link-ul din nota de subsol.[4]

Nume	Simbol	Capitalizare de piață (cf.23 aug. 2023)	Comparabil cu produsul intern brut al țărilor de mai jos[5]
Bitcoin	BTC	$514,912,135,787	Sudan
Ethereum	ETH	$201,475,414,760	Haiti
Tether USDt	USDT	$82,835,552,223	Somalia
BNB	BNB	$33,285,580,473	Andorra
XRP	XRP	$27,991,699,189	Curacao
USD Coin	USDC	$26,005,195,827	Lesotho
Cardano	ADA	$9,357,776,591	St. Vincent și Grenadine
Dogecoin	DOGE	$8,965,846,112	Insulele Mariane de Nord
Solana	SOL	$8,792,761,272	Samoa
TRON	TRX	$6,938,358,042	Samoa Americană

Pseudomonede și monede cu protecție a confidențialității

Monedele pseudo-anonime implică conturi care folosesc pseudonime, ceea ce înseamnă că, deși tranzacțiile nu sunt direct legate de date personale de identitate, unele informații de identificare rămân înregistrate. De exemplu, un cont bancar tipic în valută FIAT, utilizat pentru a cumpăra criptomonede, deține date identificabile. La această categorie se încadrează monedele Bitcoin și Ether.

În schimb, monedele cu protecție a confidențialității (privacy coins) oferă un anonimat sporit datorită utilizării metodelor criptografice pentru a ascunde detaliile tranzacției și identitățile asociate, ceea ce face dificilă trasabilitatea lor până la utilizatorul inițial. Exemple de astfel de monede sunt Monero și Zcash.

4 All cryptocurrencies (2023) CoinMarketCap./Toate criptomonedele (2023) CoinMarketCap. Disponibil la: https://coinmarketcap.com/all/views/all/ (accesat la 24 august 2023).

5 În baza datelor Băncii Mondiale privind PIB-ul (în dolari SUA), https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=false (accesat la 23 august 2023).

Portofele cripto

Un portofel de criptomonede reprezintă un loc în care sunt depozitate criptomonedele. O analogie utilă este să ne imaginăm cum sunt depozitați banii la nivel global în prezent.

Banii există în diferite forme. O parte din ei sunt depozitați în lingouri de aur, găzduite de bănci mari, o altă parte circulă sub formă de bancnote de hârtie, transferuri bancare online sau criptomonede.

Portofelele de criptomonede există, de asemenea, în diferite forme: ca aplicație pe telefon, ca dispozitiv asemănător unui stick USB, sau ca software (asemănător unei adrese de e-mail), la care puteți avea acces după ce sunt introduse numele de utilizator și parola. Deși există diferite tipuri de portofele de criptomonede, acestea folosesc aceeași tehnologie. Majoritatea au parole de recuperare din 12, 18 sau 24 de cuvinte care pot redeschide portofelul.

Adrese de portofele cripto

Adresele portofelelor de criptomonede sunt similare cu un număr de cont bancar. A cunoaște numărul de cont bancar al cuiva nu înseamnă a avea acces la banii acestuia. Adresele portofelelor cripto conțin secvențe lungi și complicate de caractere, cu multe litere și numere sensibile la majuscule și minuscule. Iată două exemple:

Un portofel de criptomonede pentru moneda TRON
TYm3NTSyk85t9UHSd68DY4vGWQADHXpaXJ

Un portofel de criptomonede pentru Bitcoin
Bc1qu5z7kn0v2krhglsnan4c0m5f76xk69p53wjwgh

Diferența dintre numărul tradițional de cont bancar și adresa de portofel cripto constă în faptul că, spre deosebire de cea din urmă, un număr de cont bancar poate oferi multe informații. Organele de aplicare a legii pot decoda cu ușurință un număr IBAN și contacta autoritatea relevantă.

Un IBAN este un număr de cont bancar internațional. Poate avea până în 34 de litere și cifre. La început este menționat codul țării, următoarele două cifre reprezintă un cod de verificare și apoi sunt trecute detaliile despre bancă și cont. În anumite cazuri, unele țări utilizează formate diferite pentru aceste detalii bancare. De exemp

IBAN:

- **LT44 32500 47338696265**

  LT identifică Republica Lituania,

  32500 identifică Revolut Bank UAB

  47338696265 este numărul de cont al utilizatorului[6]

Dacă un astfel de număr de cont bancar IBAN apare într-o investigație, ofițerul ar ști că trebuie să contacteze Banca Lituaniană Revolut. Aceste informații pot fi obținute de la așa-numiții „validatori IBAN”, cum ar fi iban.com sau https://wise.com/gb/iban/checker. Ulterior poate fi inițiat procesul de obținere a datelor personale ale utilizatorului contului. În cazul criptomonedelor pseudoanonime, cum ar fi Bitcoin, niciun organ de aplicare a legii nu va putea identifica datele personale ale titularului contului în baza unui număr de cont ca acesta: bc1qu5z7kn0v2krhglsnan4c0m5f76xk-69p53wjwgh.

Pentru a afla informațiile de identificare ale proprietarului este nevoie de un software specializat, și anume de un **furnizor de analize blockchain**.

Furnizorii de analize blockchain pot dezvălui informațiile de identificare ale utilizatorilor și pot urmări tranzacțiile dintre diferite criptomonede, o tactică comun utilizată în cazul criptomonedelor furate. Capacitatea acestor furnizori de a identifica care dintre instituțiile financiare sau platformele de tranzacționare a criptomonedelor (VASP-uri – furnizori de servicii de active virtuale) dețin aceste informații cu privire la identitate depinde

6 Codurile IBAN și ale instituțiilor financiare, Banca Lituaniei, https://www.lb.lt/en/iban-and-financial-institution-codes (accesat la 25 sept. 2023).

de legile țării în care operează. Din acest motiv, actori internaționali precum OSCE ajută statele participante să se alinieze la cele mai bune practici internaționale din acest domeniu.

Exploratoare de portofele cripto (instrumente de vizualizare a portofelelor cripto)

Deoarece principalele tipuri de blockchain public sunt disponibile pentru toți, oricine poate vizualiza toate tranzacțiile care au loc într-un portofel folosind un „explorator de portofel cripto".

Un explorator de portofel cripto este un motor de căutare conceput special pentru a naviga în datele blockchain. Acesta oferă informații detaliate despre blocuri individuale, tranzacții și portofele asociate. Gândiți-vă la acest instrument ca la un fel de „Google" pentru tranzacțiile blockchain.

Avertisment:

Este posibil să fie necesar un explorator de portofel diferit pentru fiecare tip de criptomonedă. O bună practică este să introduceți numele criptomonedei pe care doriți să o analizați, urmat de expresia „explorator de portofel cripto" sau „explorator blockchain", într-un motor de căutare, pentru a identifica principalii furnizori. Aceste servicii sunt, în general, gratuite.

Principalele utilizări ale exploratorilor de portofele cripto:

- **Verificarea tranzacțiilor:** Exploratorii de portofele permit utilizatorilor să verifice dacă a avut loc o tranzacție. Când cineva susține că a trimis o criptomonedă, lucrul acesta poate fi confirmat cu ajutorul unui explorator prin căutarea tranzacției, folosind ID-ul acesteia sau o adresă de portofel.

- **Audit și evidență:** Pentru persoanele sau companiile care au nevoie să păstreze evidența tranzacțiilor, exploratorii pot oferi informații detaliate despre data la care a avut loc o tranzacție, suma acesteia și adresele implicate.

- **Cercetare și analiză:** Dezvoltatorii, cercetătorii și analiștii folosesc adesea exploratorii de portofele pentru a studia starea și activitatea generală ale unui blockchain. Ei pot vedea câte tranzacții au loc, dimensiunea tranzacțiilor și multe altele.

- **Soldul portofelului:** Dacă introduceți o adresă de portofel într-un explorator, puteți vizualiza soldul unui anumit portofel de criptomonede și istoricul tranzacțiilor.

Exploratori gratuiți de portofele cripto:
Este ușor să găsiți exploratori de portofele cripto pentru fiecare tip de criptomonedă pur și simplu tastând „cel mai bun explorator de portofel de criptomonede XXX gratuit" într-un motor de căutare obișnuit pe internet.

Folosind aceste instrumente, oricine poate explora și verifica tranzacțiile de pe un blockchain, chiar și fără a deține criptomonede sau a avea cunoștințe aprofundate despre tehnologie. Așa cum putem căuta pe internet cu instrumente solide de căutare, putem căuta și pe blockchain-uri.

Schimbul de criptomonede

La fel ca și în cazul banilor „normali", este nevoie de o platformă specifică de tranzacționare pentru a schimba un tip de criptomonedă în altul sau în moneda FIAT. Există trei tipuri principale de platforme: Platforme de schimb de la egal la egal (sau P2P), schimburi centralizate (CEX) și schimburi descentralizate (DEX).

Denumirea P2P provine de la **peer-to-peer** (de la egal la egal), adică de la o persoană la alta sau, mai frecvent, de la un utilizator la altul (deoarece și persoanele juridice își pot vinde sau oferi activele). Aici utilizatorii nu cumpără de la platforma de schimb în sine, ci de la alți utilizatori. Un exemplu de astfel de schimb P2P care și-a încetat activitatea între timp a fost furnizorul finlandez numit LocalBitcoin.com.

Astfel de platforme de schimb își vând propriile active virtuale și nu corelează utilizatorii între ei.

Schimburile de la egal la egal sunt supuse regulamentului[7] CSB și CFT și necesită informații detaliate despre utilizatori. De asemenea, acestea trebuie să respecte anumite reguli în țările în care operează.

Schimburile descentralizate susțin că funcționează ca niște convertoare automate de fișiere (de ex., .doc în .pdf). Acestea sunt utilizate mai ales pentru tranzacții de tip cripto-în-cripto și mai rar pentru schimburi din FIAT în criptomonede. Fondurile implicate în schimburile descentralizate necesită suport specializat pentru a fi urmărite.

Acesta este doar vârful aisbergului. Există, de asemenea, noi tipuri de schimburi, pe lângă cele descentralizate menționate mai sus, și anume schimburile OTC, mixerele și „tumbler-ele". Aceasta este o tehnologie care evoluează rapid și care s-a dezvoltat cu scopul de a ascunde urmele tranzacțiilor utilizatorilor. Multe state participante la OSCE iau măsuri pentru a limita utilizarea unor astfel de instrumente.

Mixere și tumbler-e

Mixerele și tumbler-ele sunt servicii concepute pentru a spori confidențialitatea și anonimatul tranzacțiilor cu criptomonede. Funcția lor principală este de a amesteca fondurile diferiților utilizatori, ascunzând astfel sursa inițială a fondurilor.

7 Aceasta se aplică doar pentru schimburile de criptomonede ce operează în țările care au implementat recomandarea 15 a FATF cu privire la cererea de a introduce entitățile financiare care se ocupă de criptomonede în reglementările privind CSB și CFT.

Mixere

Acestea sunt servicii centralizate sau descentralizate care amestecă fondurile în criptomonede provenite din diverse surse pentru a le ascunde originea. Utilizatorii își trimit criptomonedele (cum ar fi Bitcoin) la un mixer, care apoi amestecă aceste monede cu monedele altor utilizatori sau cu propriile monede. Odată ce „procesul de amestecare" este finalizat, serviciul trimite suma echivalentă de monede, minus o taxă, la adresa specificată de utilizator, facând dificilă urmărirea originii monedelor. Cu toate acestea, mixerele centralizate sunt operate de o singură entitate care poate înregistra tranzacțiile. Echipa Europol EC3 oferă cursuri de demixare, disponibile doar organelor confirmate de aplicare a legii.

Servicii conexe de tip mixer în sistemul bancar tradițional

Mixerele funcționează similar cu băncile convenționale unde fondurile sunt depuse și retrase. Gândiți-vă la o instituție financiară mare în care diverși indivizi depun bani. Dacă această instituție ar agrega toate aceste depozite și apoi le-ar dispersa deținătorilor de conturi fără a specifica originea fiecărui dolar, acest lucru ar semăna cu procesul de mixing („amestecare"). Fondurile sunt supravegheate de o entitate cunoscută, cum ar fi un mixer centralizat, și, odată introduse, sunt amestecate cu altele. Principalii furnizori de analize blockchain susțin că oferă servicii de „demixare" automată sau manuală pentru majoritatea mixerelor de top, ceea ce permite analizarea tranzacțiilor implicate în aceste procese.[8]

Tumbler-e

Tumbler-ele sunt similare cu mixerele și, în multe contexte, termenii sunt folosiți ca sinonime. Scopul principal al unui tumbler este, de asemenea, de a îmbunătăți confidențialitatea unei tranzacții. Unii consideră tumbler-ele ca versiuni mai sofisticate ale mixerelor. Acestea aplică algoritmi avansați pentru a se asigura că monedele amestecate nu mai pot fi urmărite până la sursele lor originale.

Servicii conexe de tip *tumbler* în sistemul bancar tradițional

Tumbler-ele pot fi comparate cu conturile bancare din țări care sunt definite ca paradisuri fiscale sau cu băncile offshore, care au reputația de a oferi confidențialitate sporită. Astfel de bănci utilizează de obicei structuri și servicii complicate în mod special, cu scopul de a asigura confidențialitatea și protecția activelor. În domeniul criptomonedelor, tumbler-ele utilizează algoritmi matematici de ultimă oră pentru a menține anonimatul tranzacțiilor, oferind un nivel mai sofisticat de disimulare decât mixerele standard. Urmărirea unei tranzacții într-un tumbler este un proces complex și consumator de timp, dar nu imposibil.

Diferențe și asemănări

În timp ce atât mixerele, cât și tumbler-ele servesc aceluiași scop de a spori confidențialitatea tranzacției, discrepanțele dintre acestea constau adesea în metodele aplicate și nivelul lor de sofisticare. Este ca și cum am compara browse-erele simple de pe internet cu cele care oferă funcții de confidențialitate ridicată. Ambele tipuri vă permit să navigați pe internet, doar că unul dintre acestea vă oferă instrumente mai avansate pentru menținerea anonimatului.

VASP-uri și CASP-uri

Un furnizor de servicii de active virtuale (VASP) desfășoară următoarele activități:

- Facilitarea schimbului dintre active virtuale și monede FIAT;
- Facilitarea schimbului dintre una sau mai multe forme de active virtuale;
- Facilitarea transferului de active virtuale dintr-un portofel în altul,
- Furnizarea de servicii financiare legate de vânzarea activelor virtuale.

Există o serie de termeni folosiți ca sinonime atunci când vine vorba de VASP. „VASP" este un termen aprobat de Grupul de Acțiune Financiară Internațională (GAFI). Cu toate acestea, denumirea „CASP", care înseamnă „furnizor de servicii legate de criptoactive", este utilizată cel mai frecvent în UE în loc de VASP. Numărul de servicii acoperite de CASP este mai mare decât cel al VASP. Uneori se utilizează și termenii „platforme de schimb" și „brokeri", dar aceștia reprezintă doar unele dintre numeroasele tipuri de VASP-uri sau CASP-uri.

8 Autorul nu a putut confirma sau infirma aceste afirmații înainte de termenul limită stabilit pentru editarea acestei publicații.

Protocol pentru gestionarea infracțiunilor legate de activele digitale

Protocol pentru gestionarea infracțiunilor legate de activele digitale

Cele mai importante patru informații de verificat

Când o potențială victimă ajunge la o secție de poliție și susține că a fost supusă fraudei cu criptomonede, există patru informații vitale care trebuie verificate.

Tranzacțiile cu criptomonede sunt ireversibile – odată ce sunt finalizate și au intrat în blockchain, va fi nevoie de un efort semnificativ pentru a returna aceste fonduri victimei. Și totuși, cu toate că efortul este cu adevărat substanțial, nu este imposibil.

Timp

Primul element cheie este timpul. Tranzacțiile cu criptomonede nu intră întotdeauna imediat în blockchain. Adesea există un interval de timp în care fondurile sunt reținute la o bancă sau la un broker de criptomonede licențiat înainte de a fi înregistrate pe blockchain. A determina dacă aceasta este situația în cauză reprezintă primul și cel mai important pas, întrucât permite posibilitatea ca tranzacția să fie anulată.

Instituție financiară

Următorul aspect extrem de important este să întrebați victima la ce broker de criptomonede sau instituție financiară a apelat pentru a transfera moneda FIAT.

Dacă transferul a fost efectuat către un broker dintr-o jurisdicție cu risc scăzut unde instituțiile financiare au obligația de a respecta reglementările împotriva spălării banilor, există posibilitatea ca tranzacția în cauză să poată fi oprită.

Dimensiunea tranzacției

A treia chestiune foarte importantă este dimensiunea tranzacției, deoarece sumele mari de fonduri care depășesc pragul pentru combaterea spălării banilor sunt supuse verificării de către un VASP sau CASP. Dacă victima a făcut un transfer mare către o platformă de schimb licențiată, puteți să contactați acest operator și să opriți schimbul acestor fonduri în criptomonede.

Tipul de criptomonedă

În cele din urmă, ultima întrebare cheie este ce tip de criptomonedă sau activ virtual a fost achiziționat. Unele tipuri pot fi urmărite cu ușurință, cum ar fi Bitcoin. Alte tipuri de criptomonede cunoscute sub numele de monede cu protecție a confidențialității, cum ar fi Monero și ZCash, au fost concepute pentru a face urmărirea și investigațiile mai dificile, dar chiar și acestea sunt posibil de urmărit cu un anumit efort.

Dacă tranzacția din contul bancar al victimei s-a efectuat recent, ar trebui depuse toate eforturile pentru a o opri înainte să intre în blockchain. Atunci când un astfel de caz este raportat la secție și e transmis mai departe pentru verificare preliminară altor colegi care ar putea să-l preia câteva zile mai târziu, șansele de succes sunt reduse semnificativ.

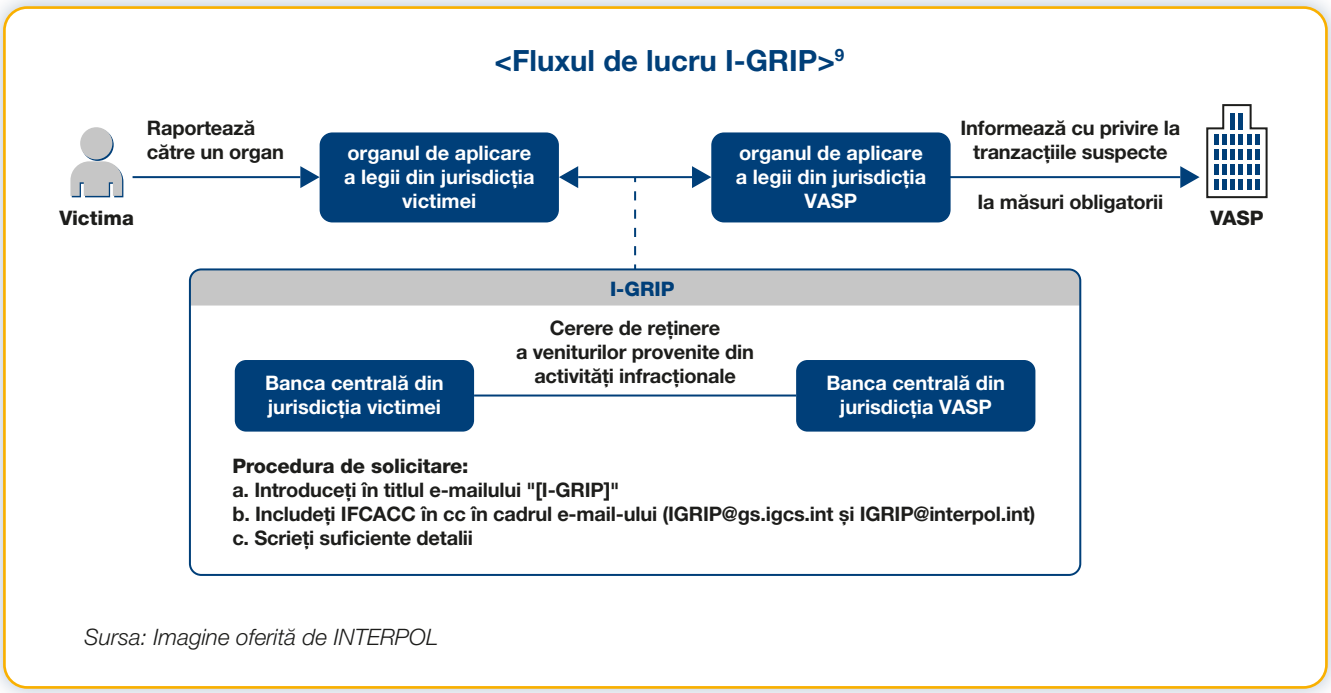
Iată trei exemple comune și ilustrative ale acestui concept:

Exemplul 1: Dacă în cazul unei potențiale victime, transferul FIAT de la o bancă internațională este inițiat, de exemplu, vineri seara, și raportat autorităților de aplicare a legii sâmbătă dimineață, atunci este încă posibil să fie contactată banca și oprită tranzacția. Dacă victima nu a contactat banca, este recomandabil să facă acest lucru imediat.
(vedeți soluția IGrip a INTERPOL, p. 23)

Exemplul 2: Chiar dacă victima a transferat o sumă mai mare din contul său bancar unui broker de criptomonede și fondurile au părăsit deja contul victimei, ar putea exista informații în contul bancar al clientului care indică denumirea VASP/CASP către care a fost efectuat transferul. În acest exemplu, dacă transferul a fost trimis către unul dintre brokerii mai mari, cum ar fi Binance, clientul ar trebui să contacteze imediat prin chat serviciul de asistență pentru clienți sau să trimită un e-mail cu titlul: **“Urgent: Stop exchange – fraud”** („Urgent: Opriți schimbul – fraudă”) către fraud@nameofthebroker.domain sau compliance@nameofthebroker.domain pentru a-i informa că transferul provenit de la un anumit IBAN, de o anumită dimensiune și efectuat într-un anumit interval orar nu trebuie procesat.

Angajații organelor de aplicare a legii pot, de asemenea, solicita blocarea fondurilor prin intermediul Sistemului Binance pentru solicitări din partea autorităților guvernamentale și organelor de aplicare a legii: https://www.binance.com/en/support/law-enforcement.

Brokerii sau platformele de schimb mai mari și alte VASP-uri au de obicei o procedură stabilită care poate ajuta organele de aplicare a legii să localizeze și să blocheze transferul. Majoritatea actorilor din domeniul dat au adrese de e-mail precum:



Sursa: Imagine oferită de INTERPOL

compliance@denumirea-brokerului.com sau fraud@denumirea-brokerului.com care pot fi utilizate pentru a raporta cazuri urgente.

În același timp, organul de aplicare a legii din jurisdicția victimei poate emite o cerere de blocare a plății prin intermediul INTERPOL, și anume cu ajutorul unui instrument numit **Global Rapid Intervention of Payment** (I-GRIP), adică „Intervenție globală rapidă a plăților". Acesta este un canal de comunicare cu organul de aplicare a legii din jurisdicția în care se află VASP-ul. INTERPOL a lansat I-GRIP pentru a accelera cooperarea internațională, astfel încât să se poată realiza etapele inițiale de recuperare a activelor.

Odată ce organul de aplicare a legii din jurisdicția în care se află VASP-ul primește o solicitare pe canalul I-GRIP, acesta poate aplica măsurile necesare pentru a împiedica procesarea în continuare a produselor infracționale, în conformitate cu legislația națională în vigoare. Măsurile necesare pot fi de diferite tipuri. Receptorul VASP poate fi pur și simplu informat despre tranzacția suspectă și acesta, ulterior, poate lua în mod voluntar decizia de afaceri de a ordona suspendarea contului suspect sau chiar revocarea tranzacțiilor. De asemenea, organul de aplicare a legii își poate folosi puterea administrativă pentru a ordona VASP-ului să suspende contul suspect. Suplimentar, organul de aplicare a legii își poate deschide propria anchetă penală internă în paralel cu ancheta desfășurată de statele care au solicitat I-GRIP și poate emite un ordin penal de sechestru asupra contului suspect.

Dacă cadrul legislativ din statul participant la OSCE permite acest lucru, o altă posibilitate ar fi înregistrarea imediată a cazului împreună cu plângerea formulată de potențiala victimă, deoarece timpul este unul dintre cele mai importante aspecte în investigațiile privind criptomonedele.

Exemplul 3: Dacă potențiala victimă nu este pe deplin sigură către ce broker de criptomonede au fost trimise fondurile și în detaliile transferului există grupuri de litere și cifre care arată similar cu șirul de mai jos:

1C5Eu4UpeK5djG3QiKwhcLELtFwHT146dG,

acest lucru ar putea indica faptul că fondurile au fost sau vor fi schimbate într-un portofel de criptomonede. Astfel de portofele pot fi corelate cu conturile bancare sau cu o căsuță poștală de e-mail, unde sunt stocate fondurile. Cu puțină abilitate, fondurile dintr-un astfel de portofel pot fi recuperate sau blocate. Chiar dacă o astfel de combinație de litere și cifre pare neobișnuită pentru persoanele care nu sunt familiarizate cu criptomonedele, pentru investigatorii cu experiență în domeniu, astfel de combinații de litere și numere furnizează informații similare cu un număr de card de credit. O adresă de portofel pentru criptomonede este similară cu un număr de card de credit, însă fără detalii personale asociate, cum ar fi numele sau banca emitentă. Un număr de card de credit indică emitentul cardului și tipul cardului. În mod similar, odată ce o victimă sesizează organul de aplicare a legii în legătură cu o adresă de portofel de criptomonede, există posibilități (care însă nu întotdeauna garantează succesul) de a conecta adresa de portofel cu o anumită criptomonedă sau cu un anumit VASP sau intermediar financiar, aplicând în acest scop niște instrumente externe.
(Pentru mai multe informații, consultați secțiunea „Instrumente suplimentare pentru investigarea infracțiunilor cu active virtuale", p. 47.)

9 INTERPOL, Guidelines for Seizing Virtual Assets (October 2023), p. 40./ INTERPOL, Ghid cu privire la sechestrarea activelor virtuale (octombrie 2023), p. 40.

Cele mai bune practici pentru fiecare tip de tranzacție

Există trei tipuri de tranzacții pe blockchain-uri, relevante pentru investigatori și pe care aceștia trebuie să le cunoască, deoarece ar putea avea nevoie să coopereze cu furnizorii de servicii de active virtuale (VASP).

Tipul tranzacțiilor	Descriere	Impactul asupra anchetei
Monedă FIAT în criptomonedă	O victimă a efectuat o plată (prin transfer bancar, plată cu cardul, plată mobilă sau în numerar) în moneda națională către un VASP care schimbă fonduri în criptomonede.	**Cea mai bună practică nr.1** **Încercați să opriți sau să anulați transferul către un broker de criptomonede, dacă este posibil.** Cel mai mare eșec în etapa de primire a sesizării este legat de înregistrarea infracțiunii suspecte și desemnarea unei persoane din cadrul secției pentru a efectua verificarea preliminară. Acest lucru întârzie contactul inițial cu victima. Dacă nu ar exista nicio întârziere, tranzacția ar putea fi oprită. Dacă tranzacția a fost efectuată în afara orelor de program bancar sau în weekend, există posibilitatea de a opri finalizarea transferului bancar, deoarece unele bănci procesează transferurile în următoarea zi lucrătoare. Dacă tranzacția a fost efectuată prin plata cu cardul, puteți lua legătura cu emitentul de carduri pentru a vă returna fondurile sau pentru a opri transferul plății. Un element cheie este să aflați ce instituție financiară a efectuat transferul bancar. Acest detaliu va fi reflectat în extrasul bancar. **Cea mai bună practică nr.2** **Dacă nu reușiți să opriți tranzacția, încercați să identificați la ce VASP a fost trimis transferul, cu scopul ca acesta să oprească tranzacția și să blocheze fondurile, dacă este posibil.** Dacă brokerul de criptomonede operează într-o țară cu risc scăzut care a introdus reglementările CSB/CFT pentru activele de criptomonede, atunci puteți să contactați brokerul fără întârziere și să solicitați blocarea sau returnarea fondurilor, dacă acestea nu au fost deja schimbate. Uneori, această procedură poate fi inițiată chiar de victime. Ulterior, brokerii ar putea opri schimbul fondurilor, deoarece prevederile CSB stipulează că fondurile pot fi transferate numai dacă originea lor este cunoscută și este clar către cine sunt trimise. Informarea operatorilor VASP că adresa de destinație a unui portofel de criptomonede este o înșelătorie îi va obliga pe aceștia să ia măsurile necesare pentru a opri tranzacția, date fiind reglementările în vigoare privind spălarea banilor.

Tipul tranzacțiilor	Descriere	Impactul asupra anchetei
		Deși acest lucru depinde de politicile interne de conformitate ale operatorului VASP, o blocare sau înghețare temporară a fondurilor (pentru câteva zile lucrătoare) va permite organelor de aplicare a legii sau procurorilor să intervină cu o cerere oficială de returnare a fondurilor. Acest lucru este posibil dacă se acționează rapid și brokerul de criptomonede este receptiv. Dacă ambele procese au eșuat, a treia posibilitate este să contactați VASP-ul identificat și să solicitați toate probele din bazele lor de date despre identitatea persoanei care și-a creat un cont de utilizator (deoarece există probabilitatea să fie un escroc sau identitatea să fie falsă), informațiile sale de identificare și hash-ul tranzacției.
Criptomonedă în criptomonedă	O victimă raportează o fraudă care se află exclusiv în cadrul tehnologiei blockchain, fără niciun fel de legături cu instituțiile financiare tradiționale care procesează monede FIAT. De exemplu, a avut loc o fraudă în care un utilizator a fost păcălit să cumpere un alt produs criptovalutar (cum ar fi NFT, Staking, etc.), fapt ce i-a cauzat pierderi financiare.	**Cea mai bună practică nr.1** **Căutați potențiali intermediari financiari autorizați, așa-numitele „platforme de tranzacționare centralizate” care au fost implicate în proces. Dacă reușiți să le găsiți, puteți colecta datele de identitate despre părțile implicate prin intermediul lor.** **Cea mai bună practică nr.2** **Adesea, victimele au fost supuse ingineriei sociale, situație care lasă multe urme ce țin de securitate cibernetică. De exemplu, suspecții cer adesea victimelor să se conecteze cu ei prin intermediul aplicațiilor pentru controlul de la distanță al ecranelor, prin e-mailuri, apeluri telefonice, transferuri bancare inițiale, sms-uri sau mesaje prin aplicații de comunicare instantanee.** În acest scenariu, victimele de regulă sunt familiarizate cu finanțele pe bază de blockchain. O primă sarcină ar fi să se colecteze cele mai precise și actualizate informații referitoare la transfer: timpii de tranzacționare, tipurile de monede utilizate de victimă, detalii despre portofelele de criptomonede, chitanțe, e-mailuri, confirmări prin sms și alte tipuri de informații. (Mai multe detalii pot fi găsite în secțiunea următoare „Colectarea probelor”, p. 27).

Tipul tranzacțiilor	Descriere	Impactul asupra anchetei
Criptomonedă în monedă FIAT	O victimă raportează furt sau pierdere de fonduri	În acest scenariu, victima deținuse criptomonede care au fost trimise către o platformă de schimb și ulterior schimbate într-o monedă națională, cel mai probabil pentru a fi extrase prin transfer bancar sau în numerar de la un sediu fizic. La fel ca în cazul transferurilor FIAT - criptomonede, aici este necesar să căutați intermediarul financiar care a efectuat schimbul în moneda națională și a inițiat transferul bancar. Dacă este implicată o sumă mare și instituția financiară este situată într-o jurisdicție cu risc scăzut, atunci această instituție trebuie să verifice de unde provin fondurile, operație efectuată de regulă manual de către angajații responsabili cu conformitatea. O astfel de verificare, în cazul în care este desfășurată, durează de obicei între 24 de ore și două zile lucrătoare de la momentul tranzacției. Dacă este posibil, introduceți adresa portofelului de criptomonede într-un explorator de portofele blockchain pentru a o verifica și a analiza dacă este legată de un intermediar financiar care ar putea fi contactat (consultați secțiunea „Instrumente suplimentare pentru investigatorii de infracțiuni virtuale”, p. 40, pentru mai multe detalii). Dacă o astfel de căutare nu are succes, atunci trebuie să utilizați un software dedicat (un furnizor de analize blockchain) care ar putea indica dacă o anumită adresă are legătură cu o instituție financiară cunoscută.

Colectarea probelor

Colectarea probelor

Colectarea informațiilor de la o persoană fizică

10 categorii de informații esențiale pentru anchetă

- **Natura activului:** ce proiect de criptomonedă sau NFT a fost implicat, inclusiv numele, simbolul și specificul tehnologiei de bază.
- **Detalii despre tranzacție:** Informații despre tranzacțiile efectuate de victimă, cum ar fi data, ora, suma, moneda și ID-urile tranzacției (de ex., chitanțele de la un VASP).
- **Adrese de portofel:** Detalii despre adresele portofelelor de criptomonede implicate, atât ale victimei, cât și ale suspectului escroc.
- **Istoricul comunicărilor:** Toate comunicările pe care victima le-a avut cu presupușii escroci, fie prin e-mail, rețele de socializare, aplicații de chat, apeluri telefonice sau forum-uri.
- **Materialele promoționale:** Toate anunțurile publicitare, postările online sau oricare alte materiale promoționale primite de victime în legătură cu activele virtuale. În ceea ce privește copiile e-mailurilor, asigurați-vă că hyperlink-urile sunt incluse în ele, în mod ideal pe stick-uri USB. Atenție! În timp ce înregistrați astfel de materiale, nu faceți clic pe niciun hyperlink furnizat în materialul electronic, deoarece acestea ar putea fi virusate.
- **Detalii despre platformă:** Toate detaliile despre platforma sau schimburile operate de VASP-ul (vedeți secțiunea „VASP-uri și CASP-uri”, p. 20) de la care victima a achiziționat activul în criptomonede. Pentru informații despre cum să solicitați date de la VASP, vedeți secțiunea de mai jos, „Solicitarea de date de la VASP-uri”, p. 29. Denumirile schimburilor pot fi adesea găsite pe chitanțele tranzacțiilor.
- **Informațiile cu privire la recomandări:** Informații despre modul în care victima a aflat despre activul în cauză, fie printr-o recomandare, o publicitate online, în mod direct de la cineva, etc.
- **Anomaliile de codare:** Dacă este disponibilă, orice dovadă a codului manipulat cu scopul de a împiedica vânzarea sau orice alte anomalii. Toate hyperlink-urile către sit-urile web utilizate pentru a susține infracțiunea și, în funcție de jurisdicție, atunci când victima a eliminat datele financiare, toate credențialele de autentificare care ar ajuta organele de aplicare a legii să înțeleagă modul în care funcționează software-ul utilizat.
- **Înregistrările financiare:** extrase bancare, extrase de card de credit sau alte înregistrări financiare care reflectă transferul de fonduri legate de investiție.
- **Informațiile de identitate:** Toate detaliile care pot ajuta la identificarea escrocului, cum ar fi numele de utilizator, profilurile de pe rețelele de socializare, adresele de e-mail sau oricare alte date de contact care au fost utilizate în timpul interacțiunii cu victima, pe computerul victimei.
- **Anomaliile tehnologice:** Victima a instalat aplicații software pe parcursul desfășurării înșelătoriei? Acest software a fost dezinstalat sau este încă pe computer? Este posibil să se determine sursa sau originea software-ului?

Dacă o tranzacție cu criptomonede nu a fost suspendată, este vital să obțineți adresa portofelului de criptomonede de unde au fost trimise sau primite fondurile.

Colectarea adreselor portofelelor de criptomonede

Care sunt cele mai importante informații necesare pentru o investigație pe blockchain?

Detaliile tranzacției: Adresa portofelului de criptomonede și numerele hash

O greșeală comună este înregistrarea incorectă a adreselor de portofele de criptomonede, dat fiind că acestea implică șiruri lungi de numere și litere.

Exemplul 4: Când înregistrați o adresă de portofel de criptomonede etc., cifra zero „0” poate fi ușor confundată cu litera O, sau litera q cu g. O bună practică este să introduceți adresa de portofel de criptomonede pe care doriți să o înregistrați într-un motor de căutare pe internet, cum ar fi Google sau Bing, pentru a vedea dacă poate fi identificată. Dacă adresa nu apare imediat, puteți folosi un instrument de explorare a portofelului.
(Vedeți și secțiunea „Instrumente suplimentare pentru investigatorii infracțiunilor cu active virtuale”, p. 47.)

Dacă adresa portofelului de criptomonede este corectă, vor fi afișate imediat informații care vor permite extragerea următoarelor date:

Valabil doar pentru Bitcoin:

- **Suma tranzacției:** Puteți vedea suma de Bitcoin care a fost trimisă sau primită în fiecare tranzacție.
- **Ora tranzacției:** Este vizibil un marcaj temporal care indică momentul în care o tranzacție a fost inclusă într-un bloc.
- **Soldul curent al portofelului de criptomonede:** Puteți vizualiza suma totală de Bitcoin prezentă în portofel.
- **Hash-ul tranzacției:** Acesta este un identificator unic pentru fiecare tranzacție, un fel de ID de tranzacție utilizat de furnizorii de servicii de plată care servește drept „amprentă".

Disponibil la unele servicii, dar nu la toate:

- **Volumul tranzacției:** Unele servicii oferă detalii despre volumul tranzacției, adesea schimbat în monede FIAT principale, cum ar fi USD sau EUR.
- **Personalizarea fusului orar:** Anumite platforme oferă posibilitatea de a modifica fusul orar, care implicit este UTC. De exemplu, utilizatorii îl pot ajusta la fusul orar local, ceea ce ajută la colectarea probelor.

Este posibil ca o adresă de portofel de criptomonede să stocheze diferite tipuri de criptomonede?

Posiblitatea ca un utilizator să folosească o singură aplicație pentru a accesa diverse active virtuale cu aceleași date de autentificare este încorporată în portofelul multi-signature (MultiSig). MultiSig utilizează o singură aplicație pentru a gestiona diverse active virtuale cu aceleași credențiale, simplificând procesul de gestionare a diferitelor criptomonede.

Așa cum băncile atribuie numere de cont unice pentru diferite valute – unul pentru USD, altul pentru EUR – criptomonedele bazate pe diferite tehnologii blockchain, precum Bitcoin și Tron, necesită adrese unice de portofel.

Portofelele MultiSig nu implică neapărat mai multe persoane; în schimb, necesită utilizarea mai multor chei private pentru a autoriza o tranzacție. O persoană ar putea deține mai multe chei private sau mai multe persoane ar putea fi implicate în gestionarea activelor, fiecare cu propria cheie privată.

O vizualizare a acestui concept poate fi reprezentată de distincția dintre tipurile de smartphone-uri și sistemele sau aplicațiile pe care le acceptă. Anumite aplicații sunt concepute exclusiv pentru iOS de la Apple și necesită un iPhone, în timp ce altele sunt adaptate pentru Android și nu vor funcționa pe dispozitivele Apple. Cu toate acestea, pe platforma Android pot rula diverse aplicații dezvoltate de diferiți programatori și pot fi obținute din Magazinul Google Play. În mod similar, criptomonedele unificate de o tehnologie comună, cum ar fi jetoanele ERC20 construite pe blockchain-ul Ethereum, pot fi gestionate într-o singură adresă de portofel bazată pe Ethereum.

Acest lucru reflectă modul în care un singur magazin de aplicații facilitează descărcarea a numeroase aplicații dezvoltate pe aceeași platformă. De asemenea, criptomonedele dezvoltate pe același blockchain, cum ar fi Ethereum, pot fi consolidate într-o singură adresă de portofel bazată pe Ethereum, permițând o experiență de utilizator mai eficientă.

Solicitarea datelor de la VASP-uri

Dacă victima nu știe cărui furnizor de servicii de active virtuale (VASP) au fost trimiși banii, este posibil să aibă o chitanță care să arate adresele portofelului. Dacă nu, aceste date pot fi adesea vizibile folosind un software de analiză blockchain. Astfel de furnizori sunt înregistrați în țări în care legile prevăd în mod clar că activele virtuale trebuie să respecte normele de combatere a spălării banilor. Conform acestor reguli, VASP-urile trebuie să verifice identitatea utilizatorilor lor și să țină evidența tranzacțiilor. De exemplu, în Uniunea Europeană, conform celei de-a cincea Directive CSB, VASP-urile din statele membre UE trebuie să fie înregistrate și să respecte o varietate de obligații privind combaterea spălării banilor.

Dacă victima știe către ce sau de la care VASP au fost trimise/au venit fondurile și încă deține (sau poate recupera) datele de autentificare, atunci primul pas este să extragă de la respectiva platformă de schimb toate informațiile cu privire la transferul efectuat. Aceste informații legate de transfer vor include tranzacțiile efectuate, criptomonedele trimise și adresele lor de portofel.

Dacă victima nu este sigură de unde au fost transferate fondurile sau unde au fost trimise, denumirea VASP poate fi găsită uneori pe extrasul bancar sau pe extrasul de card al victimei.

Unele dintre denumirile activelor virtuale sau ale schimburilor includ PanCake Swap (https://pancakeswap.finance/); Wasabi Wallet (https://wasabiwallet.io); Doge Coin (https://dogecoin.com/); și Shit Coin (https://www.investopedia.com/terms/s/shitcoin.asp). Deși aceste denumiri nu sună familiar celor care nu activează în lumea criptomonedelor, ele sunt utilizate în mod obișnuit.

Chiar și platformele care pretind că sunt complet descentralizate, cum ar fi Uniswap, oferă posibilitatea de vizualizare al istoricului tranzacțiilor pentru utilizatorii în format.csv, ceea ce poate ajuta la o investigație.

Cu sute de platforme centralizate de tranzacționare în întreaga lume, doar câteva nume ar putea fi ușor de recunoscut de publicul larg sau de organele legii.

Dacă o persoană nu poate recupera accesul la contul său pe o platformă VASP, este posibil să apeleze la un VASP centralizat sau la un portofel de criptomonede (furnizor de custodie) pentru ajutor.

Conform bunelor practici, VASP-urile nu vor furniza, de obicei, nicio informație prin telefon, deci este nevoie de o Cerere Oficială din partea Organelor de Aplicare a Legii (Law Enforcement Request) către VASP sau alte instituții financiare care au procesat fondurille victimei. Procesul de completare a unei astfel de interpelări la un VASP este descris la pagina 22.

Cel mai probabil veți primi următoarele informații de la un VASP centralizat:

- Prenume
- Nume
- Data nașterii
- Copii ale actelor de identitate[10]
- Anvergura tranzacțiilor finalizate
- Data și ora (marcajul temporal) al tranzacțiilor[11]
- Tipul tranzacției (FIAT și criptomonedă)[12]
- Valoarea comisionului agentului
- Ora confirmării verificărilor privind sancțiunile și persoanele expuse politic și tipurile de liste de supraveghere care au fost utilizate.
- **Adresa portofelului de criptomonede, eventual,** adresele, dacă există mai multe tranzacții și valute
- Hash-uri ale tranzacțiilor efectuate

Este mai puțin probabil, dar totuși posibil să primiți următoarele informații:

- Numărul de client sau ID-ul înregistrat în cadrul agentului
- Domiciliul declarat[13] al clientului
- Domiciliul înregistrat al clientului[14]
- Numărul de asigurare socială, în funcție de țară în care este înregistrată platforma
- Interacțiuni între agent (VASP/CASP) și client (adesea sub forma unui fișier PDF, deoarece serviciul pentru clienți este adesea realizat de către furnizori externi de software, cum ar fi Intercom sau ZenDesk)
- Toate documentele care oferă dovada fondurilor – încărcate către și de la utilizatori
- Adresa IP (care ar putea fi înșelătoare, deoarece utilizatorii tind să folosească VPN-uri)
- Dispozitiv utilizat pentru autentificare, cum ar fi un telefon mobil sau un computer desktop
- Browserul și versiunea utilizată pentru accesarea serviciului: Opera, Chrome, Safari, Internet Explorer sau similar
- Verificări ale antecedentor clientului, efectuate utilizând informații din surse deschise (Open Source Intelligence, OSINT)[15]
- Observațiile angajaților VASP cu privire la un anumit utilizator sau tranzacțiile acestuia
- Orice investigații analitice pe blockchain efectuate asupra utilizatorului sau a tranzacțiilor acestuia de către angajații VASP
- Orice solicitări de informații despre utilizatorul respectiv de la alte organe de aplicare a legii sau instituții financiare
- Orice tranzacție inițiată de utilizator, dar nefinalizată
- În cazul birourilor fizice sau al ATM-urilor, pot exista înregistrări video cu persoanele care utilizează locația
- Solicitați toate documentele încărcate de utilizatori (inclusiv informații ce adeveresc sursa fondurilor și averiii), precum și toate interacțiunile cu serviciul clienți

Ofițerii de poliție pot colecta informații suplimentare de la victimă privind detaliile contului său bancar, ceea ce poate ajuta la filtrarea informațiilor obținute de la VASP-uri. Aceste informații sunt disponibile numai pentru tranzacțiile FIAT în cripto (nu și pentru tranzacțiile cripto în FIAT).

- Numărul de cont bancar al victimei care a fost utilizat pentru a efectua un transfer către și dinspre un cont VASP.
- Număr de telefon: unii utilizatori folosesc sistemul de plată al telefonului mobil.
- Informații despre cardul de credit, debit sau cel preplătit, utilizate

10 Aceasta poate include un pașaport, o carte de identitate sau un act de identitate electronic. Însă această procedură are aceleași vulnerabilități ca și în cazul infracțiunilor cibernetice tradiționale, cum ar fi utilizarea de documente false sau de colecție care imită documente de identitate reale (de exemplu, „documente de colecție" disponibile pe site-uri precum dokumencik.pl).

11 Este important să determinați la ce fus orar se referă marcajul temporal. De exemplu, toate tranzacțiile blockchain Bitcoin sunt înregistrate cu UTC (ora Londrei) indiferent de locul din care provine utilizatorul. Uneori, problematica corelării marcajelor temporale incorecte ale tranzacțiilor cu alte probe devine critică.

12 Atât activele virtuale, cât și FIAT.

13 Dacă legislația țării permite, se poate verifica dacă sunt și alți clienți ai platformei care au efectuat tranzacții și care sunt înregistrați la aceeași adresă.

14 Dacă platforma extrage astfel de informații dintr-o bază publică de date.

15 Aceasta ar putea include extrageri din surse de date disponibile public, cum ar fi certificate de cazier judiciar sau informații despre beneficiarii finali ai anumitor întreprinderi - informații care ar fi putut fi extrase de angajații unității de conformitate a platformei.

pentru efectuarea tranzacției. Contul furnizorului poate conține informații suplimentare, cum ar fi un al doilea nivel de confirmare printr-o aplicație bancară mobilă sau serviciul SMS numit 3D secure, care poate fi obținut

- Pentru țările care utilizează sistemul de „open banking" (servicii bancare deschise), pot fi disponibile informații suplimentare de la furnizorii de servicii de plată care procesează aceste tranzacții (dacă tranzacțiile respective au fost finalizate folosind open banking)

Formatul informațiilor pentru datele VASP

Pentru a asigura o eficiență optimă, este recomandat să obțineți datele tranzacționale necesare într-un format „.csv", facilitând integrarea directă în sistemele forțelor de ordine. De obicei, răspunsurile la solicitările oficiale din partea organelor de aplicare a legii (LER) sunt oferite în două formate:

- Un fișier „.pdf" în care furnizorul de active virtuale oferă răspunsuri directe la întrebările adresate de organele de aplicare a legii (LEA)

- Un fișier „.csv" cu date despre tranzacție

Adesea, VASP-urile păstrează un dosar cu date consolidate ale clienților. Acest dosar include documente importante, cum ar fi dovada fondurilor (Proof of Funds -POF) și alte fișiere încărcate. VASP-urile mari au, de obicei, o metodă standardizată de a răspunde solicitărilor din partea organelor de aplicare a legii. Atunci când interacționează cu instituții mai mici, autoritățile pot specifica formatul de date preferat pentru primirea informațiilor solicitate.

Cu toate acestea, identitatea clientului poate fi uneori transmisă în diverse formate, cum ar fi un fișier „.pdf" sau „.jpeg" al unui document de identitate sau un videoclip care există în formate precum „.avi" sau „.mov".

Este recomandat să evitați solicitarea fișierelor „.xml" sau „.xls" de la VASP-uri. Mai exact, utilizarea fișierelor „.xlsx" nu este recomandată din cauza riscurilor asociate cu securitatea cibernetică. Există riscul ca datele furnizate de VASP-uri în format „.xlsx" să conțină viruși, în special în macrocomenzile încorporate în fișier, ceea ce poate compromite securitatea sistemelor informatice ale organelor de aplicare a legii.

Fiabilitatea adreselor IP obținute

O adresă IP (IP) poate fi adesea obținută de la un VASP printr-o procedură oficială din partea organelor de aplicare a legii. Adresa IP este un identificator unic al unui dispozitiv precum un smartphone sau un laptop, conectat la rețeaua de internet. Gândiți-vă la o adresă IP ca la un set unic de numere, cum ar fi un număr de telefon. De exemplu, 193.46.242.201 indică Stockholm, Suedia. Dar, la fel cum un număr de telefon fix poate fi folosit de mai mulți membri ai familiei în aceeași casă, mulțumită tehnologiei numite NAT (Network Address Translation), mai multe dispozitive pot folosi aceeași adresă IP.

VASP-urile susțin adesea că pot exporta adrese IP care au fost captate în timpul autentificării utilizatorilor, însă fiabilitatea acestor informații pentru investigații ar trebui să fie pusă sub semnul întrebării. Adresele IP indică doar ce dispozitiv a accesat internetul, nu și cine l-a folosit în mod specific. Aceste informații pot fi camuflate de escroci care folosesc rețele private virtuale (VPN) și, prin urmare, ar trebui utilizate numai în cazurile în care există alte probe care pot corela IP-ul utilizatorului cu o potențială activitate infracțională.

Companiile care oferă acces la internet pentru utilizatorii casnici (numite furnizori de servicii de internet, „ISP") pot identifica adesea cine a folosit o anumită adresă IP la un moment dat. Pe parcursul unei investigații, acestor companii li se poate solicita să coreleze adresa respectivă cu anumiți utilizatori care au semnat un contract de furnizare a serviciillor respective. Din păcate, chiar dacă utilizatorul nu folosește VPN, aceste informații nu sunt întotdeauna de încredere. Utilizatorii își pot pune la dispoziție rețelele WiFi fără parolă, ceea ce înseamnă că alte persoane pot folosi acea conexiune și, implicit, acea adresă IP.

Cunoașterea unei adrese IP nu oferă întotdeauna informații exacte despre cine a efectuat o anumită acțiune online. În medii precum birouri publice, școli sau locuri de muncă, mai multe persoane ar putea utiliza aceeași conexiune la internet, complicând și mai mult atribuirea acțiunilor online unei anumite persoane.

În cele din urmă, VPN-urile sunt concepute pentru a ascunde adresa IP reală a unui utilizator, simulând faptul că originea conexiunii se află într-o locație diferită.

Cu toate acestea, chiar și cu un VPN ar putea exista posibilitatea de a corela anumite comportamente ale utilizatorului cu vizitarea anumitor site-uri web, asociindu-le cu un anumit IP într-un anumit interval de timp. Acest lucru înseamnă că, deși VPN-urile contribuie la creșterea anonimatului utilizatorilor, ele nu fac ca acțiunile online să fie complet imposibil de urmărit. Totuși, în anumite circumstanțe, entitățile ce au capacitatea de a efectua analize aprofundate ar putea să stabilească o legătură între activitățile online și utilizatorii individuali.

Colectarea adreselor IP

Argumente pro:

- **Trasabilitate:** Adresele IP pot servi drept punct de pornire pentru a urmări potențialii suspecți sau pentru a identifica originea activităților suspecte. Există posibilitatea ca aceste informații să poată fi asociate cu alte investigații.

- **Descurajare:** Odată ce află că adresele lor IP sunt monitorizate, persoanele cu intenții infracționale pot fi descurajate să utilizeze propriile rețele pentru desfășurarea de activități ilicite.

Roman Bieda conduce un atelier practic pentru anchetatorii din Kazahstan. În calitate de fost proprietar al unui instrument de analiză blockchain și martor expert în instanțele din Europa și Statele Unite, el se concentrează pe împărtășirea nu numai a cunoștințelor, ci și a celor mai bune practici și perspective cu privire la provocările cu care se confruntă în timpul procesului de colectare a probelor. Scopul atelierelor OSCE este de a se asigura ca provocările întâmpinate într-un stat participant nu se vor repeta în altele.

- **Coroborarea cu alte probe:** Coroborate cu alte probe, adresele IP pot ajuta la consolidarea unui dosar mai solid împotriva suspecților.

Argumente contra:

- **Inexactitate:** Deoarece mai multe dispozitive pot utiliza o singură adresă IP și, având la dispoziție VPN-uri și alte instrumente de ofuscare, bazarea exclusivă pe adresele IP poate duce la identificări eronate.

- **Preocupări legate de confidențialitate:** Colectarea adreselor IP în masă poate încălca drepturile de confidențialitate ale persoanelor, mai ales dacă aceasta se face fără o justificare solidă.

- **Utilizarea intensivă a resurselor:** Urmărirea și verificarea adreselor IP, în special în contextul utilizării VPN-urilor sau altor instrumente de mascare, pot consuma mult timp și pot deturna resurse de la alte activități importante de investigație.

În concluzie, deși adresele IP pot oferi informații suplimentare despre activitatea unui dispozitiv și locația unui anumit dispozitiv la un moment dat, ele nu identifică în mod concludent utilizatorii individuali. Investigațiile bazate pe adresele IP sunt utile numai atunci când sunt abordate cu prudență și se consideră drept parte a unui instrumentar mai larg.

Alte documente de solicitat

În unele state participante la OSCE, companiile care gestionează active virtuale (cum ar fi criptomonedele) sunt considerate „instituții financiare supuse obligațiilor legale” sau intermediari. Aceasta înseamnă că ele trebuie să monitorizeze în mod regulat activitățile clienților lor. Companiile sunt obligate să analizeze clienții și tranzacțiile ce prezintă un comportament suspect, adesea folosind instrumente de analiză blockchain pentru a identifica potențialele surse de risc. Odată ce aceste verificări sunt efectuate și documentate, organele de aplicare a legii pot solicita să le vadă.

De exemplu, în Republica Georgia, furnizorii serviciilor tip platforme schimb care sunt înregistrate la Banca Națională a Georgiei sunt obligate să utilizeze instrumente specializate pentru a analiza tranzacțiile blockchain. Aceasta asigură un nivel de transparență și securitate în monitorizarea fluxului de active virtuale.

Dacă organele de aplicare a legii nu au acces la astfel de instrumente de analiză blockchain, ele pot solicita VASP-urilor să furnizeze detalii relevante pentru investigație. **Aceste informații pot fi transmise într-un format accesibil și editabil, cum ar fi un fișier PDF sau o imagine.**

Aceasta înseamnă că, deși instrumentele sunt esențiale în menținerea integrității tranzacțiilor și în identificarea activităților ilegale, există considerente procedurale și juridice care trebuie respectate atunci când se transmit informații obținute prin intermediul lor. De exemplu, mai mulți furnizori de servicii de analiză blockchain și de soluții de conformitate ar putea avea protocoale și acorduri specifice care limitează transmiterea de informații sensibile sau editabile chiar și către organelor de aplicare a legii fără autorizație prealabilă. Aceasta poate genera dificultăți pentru VASP-urile, care pot fi reticente să dezvăluie informații fiabile în detrimentul obligației de a restricționa accesul la dovezi din cauza constrângerilor impuse de aceste acorduri.

Trimiterea cazurilor în instanță

Trimiterea cazurilor în instanță

Procurorii cazurilor privind activele virtuale

Pentru a asigura o bază solidă de lucru pentru procurori, ofițerii de aplicare a legii ar trebui să fie bine pregătiți în colectarea probelor legate de activități de combatere a spălării banilor (CSB), în special în cazul activelor virtuale și al criptomonedelor, un domeniu ce este în continuă expansiune.

Etapa de investigație

- **Căutați probe digitale:** Înțelegeți și monitorizați tranzacțiile pe blockchain și registrele distribuite.
- **Analizați informațiile:** Recunoașteți tipare care ar putea sugera spălarea banilor, cum ar fi tranzacțiile rapide și cu un volum mare, trecute prin schimburi de criptomonede.
- **Urmați indiciile digitale:** urmăriți fluxul activelor prin mai multe portofele și platforme virtuale, utilizând software specializat dacă este necesar.
- **Evaluați credibilitatea tuturor informațiilor de identificare** primite de la VASP-uri (vedeți provocările legate de „Copii ale documentelor de identitate”, p. 30)

Pregătirea materialelor pentru instanță sau pentru investigație

a. Prezentare generală a cazului:

- Ar trebui să se pună accent pe portofelele cripto, adresele IP, marcajele temporale ale tranzacțiilor și sumele tranzacționate digital.
- Primul obiectiv ar trebui să fie înțelegerea conversiei activelor virtuale în active corporale, cum ar fi proprietăți sau bunuri, și urmărirea originii acestora.

b. Identificarea tipului de infracțiune:

- Recunoașterea semnelelor utilizării criptomonedelor pentru spălarea banilor, cum ar fi prin servicii de „tumbling” sau „mixing” (mixare) care urmăresc să ascundă sursa fondurilor. Unii dintre cei mai importanți furnizori de analiză blockchain oferă „servicii de demixing” (demixare) care pretind că pot descompune tranzacțiile care au fost procesate printr-un mixer. Dacă cazul este de importanță majoră, există atât servicii de demixare oferite de furnizorii de analize blockchain, cât și cursuri despre demixare oferite de organele de aplicare a legii precum Europol.
- Utilizați registrul tranzacțiilor blockchain pentru a proba elementele constitutive ale infracțiunii.

c. Legătura dintre activitatea infracțională și active:

- Urmăriți orice mișcare de fonduri din portofelele cripto până la achiziționarea de active corporale sau alte active virtuale. Acest lucru ar putea implica analizarea mișcărilor cripto de la platforme de tranzacționare la un portofel privat și apoi la o altă entitate sau serviciu.
- Identificați orice servicii sau tehnici de anonimizare utilizate și încercați să urmăriți activele în ciuda acestor provocări.
- Recunoașteți tipare care pot indica intenții infracționale precum spălarea banilor, cum ar fi împărțirea unor cantități mari de criptomonede în mai multe portofele sau utilizarea monedelor de confidențialitate precum Monero sau Zcash.

Prezentarea probelor:

- Explicați clar cum funcționează criptomonedele și blockchain-ul, deoarece este posibil ca instanța să nu fie familiarizată cu această tehnologie.
- Prezentați un traseu digital clar și concis al procesului de spălare a banilor, de la sursa fondurilor ilicite până la destinația lor finală. Se recomandă crearea unor materiale vizuale și utilizarea unui limbaj simplu, non-tehnic, atunci când se prezintă probe, deoarece mulți procurori sau judecători s-ar putea să nu fie încă pe deplin familiarizați cu complexitatea domeniului criptomonedelor.

Probe suplimentare:

- Înregistrări de pe platforme centralizate de tranzacționare pentru criptomonede: Acestea pot oferi detalii despre activitatea utilizatorului, adrese de portofel, jurnale IP, sume tranzacționate și datele tranzacțiilor.
- Software de analiză blockchain: Un astfel de software poate vizualiza fluxul de monede digitale.
- Examinarea portofelor digitale: Investigați portofele hardware, portofele mobile, și portofele desktop. Acestea ar putea conține înregistrări, istoricul tranzacțiilor sau metadate care pot fi utile.
- Urmărirea adresei IP: Urmăriți adresele IP asociate tranzacțiilor pentru a identifica locația geografică a suspecților. (vedeți la p. 31 limitările în utilizarea adreselor IP)
- Colaborarea cu agențiile internaționale: Datorită naturii descentralizate a criptomonedelor, cooperarea transfrontalieră este crucială pentru urmărirea tranzacțiilor transfrontaliere. Cu toate acestea, o astfel de cooperare este de obicei începută într-o etapă ulterioară de către un investigator principal.[16]

Prin colectarea de probe cuprinzătoare legate de tranzacțiile și activitățile cu criptomonede, ofițerii de poliție pot oferi colegilor implicați în investigații, precum și procurorilor, o bază solidă pentru a-și consolida dosarele și pentru a se asigura că infractorii sunt trași la răspundere.

16 Unități de informații financiare care colaborează cu Grupul Egmont au dezvoltat un mecanism de sistem de schimb care poate fi accesat aici: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf (accesat la 15 feb. 2024)

Recomandări și contacte pentru cazuri complexe

Recomandări și contacte pentru cazuri complexe

Echipe dedicate și cunoștințe speciale

Furnizorii de top de software de analiză blockchain înființează frecvent echipe dedicate, formate din experți atât în domeniul criptomonedelor, cât și în proceduri investigative. Aceste echipe se specializează în asistarea organelor de aplicare a legii în navigarea complexității analizei blockchain, asigurându-se că instrumentele sunt utilizate la potențialul lor maxim. Este recomandat să verificați intranetul instituției pentru a vedea ce departamente folosesc deja software de analiză blockchain, deoarece colegii din aceste departamente probabil vor fi cei mai familiarizați cu acest domeniu.

Instruire și certificare

Având în vedere complexitatea tehnologiilor blockchain și importanța unui management solid al cunoștințelor, mulți furnizori de software de analiză blockchain oferă, de asemenea, programe structurate de formare. Adesea, aceste cursuri se finalizează cu diferite niveluri de certificare, care nu numai că validează abilitățile personalului de aplicare a legii, ci și amplifică eficiența acestora în gestionarea investigațiilor legate de blockchain. În timp ce unele servicii, cum ar fi sprijinul de tip consultanță, pot necesita finanțare suplimentară, avantajele pe termen lung în ceea ce privește capacitățile sporite de investigare pot fi substanțiale.

Sprijin extern pentru investigații aprofundate

Pe lângă echipele interne și cursurile proprii de instruire, există și o gamă tot mai extinsă de furnizori comerciali externi, specializați în efectuarea de investigații exhaustive ale tranzacțiilor cu criptomonede pe blockchain. Acești furnizori acționează în calitate de subcontractanți, oferindu-și serviciile competente organelor de aplicare a legii. Cunoștințele lor pot fi extrem de valoroase, mai ales în cazuri complexe în care sunt necesare analize aprofundate și tehnici de investigație cu mai multe fațete. Organele de aplicare a legii, cum ar fi INTERPOL sau Europol, oferă sprijin și formare dedicate anchetatorilor (vedeți secțiunea „Cooperare cu experți în domeniul activelor digitale”, p. 51). Dacă echipa dumneavoastră dorește să participe la evenimentele de instruire disponibile, vă rugăm să contactați VirtualAssets@osce.org pentru informații suplimentare.

Acționați cu prudență

Cu toate acestea, în timp ce avantajele furnizorilor externi sunt numeroase, organele de aplicare a legii trebuie să fie conștiente și de potențialele provocări. Implicarea entităților externe în investigații sensibile, precum agențiile de consultanță sau furnizorii de servicii de analiză pe blockchain, poate complica desfășurarea proceselor judiciare. Există și problema majoră privind securitatea datelor. Transferul de informații sensibile către terți trebuie abordat cu cea mai mare precauție pentru a asigura menținerea integrității datelor și pentru a evita orice divulgare accidentală a informațiilor confidențiale.

Maciej Szulc conduce un atelier de formare a formatorilor la Gdansk, unde factorii de decizie din state participante OSCE împărtășesc cele mai bune practici pentru soluționarea cazurilor complexe și asistarea părților naționale interesate. Accentul este pus nu doar pe calitatea conținutului, ci și pe metode eficiente de livrare a materialului cursului.

Sprijin pentru victime

Sprijin pentru victime

Provocările despre care victimele ar trebui să fie avertizate

Victimele unei escrocherii cu criptomonede pot cădea cu ușurință pradă altora. Grupările infracționale organizate nu atacă doar o dată, ci își vizează victimele în mod repetat și strategic. Mai jos sunt detalii despre escrocherii secundare comune:

- Înșelătoria „salvatorului”. După ce o persoană a fost implicată inițial într-o rețea de escrocherii, o altă ramură a aceleiași structuri îi oferă, pretinzând a fi un profesionist, ajutor pentru a-și recupera investițiile pierdute: Această ofertă aparent generoasă vine cu un preț, victima fiind nevoită să plătească unei companii de servicii pentru a recupera fondurile pierdute. După ce fondurile au fost transferate, „salvatorul” dispare adesea împreună cu sumele pierdute.
- Tactica „avertizorului de integritate”: Sub o altă înfățișare, escrocii se pot comporta ca foști angajați nemulțumiți ai întreprinderii frauduloase, afirmând că dețin cunoștințe din interior care ar putea ajuta victimele să-și recupereze activele. Procesul este același ca și în cazul „salvatorului” – sumele trebuie plătite în avans și apoi persoana de contact dispare de obicei.
- Mirajul recursului legal: Acestea sunt scenarii în care victimele sunt abordate de un profesionist din domeniul juridic care promite să recupereze banii, în special atunci când sunt implicate VASP-uri. După ce victima convine asupra unui tarif orar, acești avocați susțin că au creat documente extinse, uneori peste 40 de pagini, care detaliază adesea principiile fundamentale din legislația privind combaterea spălării banilor (CSB) și a finanțării terorismului (CFT), însă au o valoare juridică limitată. Din păcate, documentele care au fost folosite sunt în mare parte generice și 99% dintre ele rămân neschimbate, astfel încât VASP-ul este inundat cu aceleași documente cu detalii personalizate nesemnificative. Victimelor li se percep tarife exorbitante pentru aceste demersuri în mare parte inutile. Este esențial să înțelegem că la majoritatea VASP-urilor, tranzacțiile, odată efectuate, sunt ireversibile. Solicitarea de rambursări prin „credit card chargebacks” (adică prin retragerea tranzacției efectuate de pe card) are șanse reduse de succes. Prin urmare, astfel de măsuri legale sunt de obicei de valoare redusă și, mai degrabă, epuizează resursele financiare ale victimei.

Olga de Truchis, expert OSCE în active virtuale și Co-Pilot al Programului Europol „Parteneriat public-privat pentru Informații Financiare cu privire la Criptoactive (EFIPPP)”, a condus o sesiune privind cele mai bune practici pentru furnizorii financiari tradiționali în gestionarea riscurilor de criminalitate financiară asociate activelor virtuale și furnizorilor de servicii de active virtuale. Atelierul, găzduit de sediul Băncii Naționale a Letoniei (Latvijas Banka), a inclus reprezentanți ai altor patru state participante la OSCE.

Tipuri de infracțiuni comise cu implicarea criptomonedei

Tipuri de infracțiuni comise cu implicarea criptomonedei

Mai jos sunt detalii despre cele mai frecvente tipuri de infracțiuni comise cu implicarea criptomonedelor. Ar trebui să fim cel puțin conștienți de aceste tipuri de infracțiuni, dar să știm că aceasta nu este o listă cuprinzătoare.

Scheme frauduloase cu investiții în criptomonede

Ce reprezintă?

Escrocheriile cu investiții în criptomonede sunt unele dintre cele mai frecvente tipuri fraudă. Inițial, această înșelătorie a vizat cetățenii în vârstă cu venituri mari din țările cu venituri ridicate. Însă tacticile au evoluat, și acum investitorii pe piața de capital și cei care se apropie de vârsta de pensionare sunt din ce în ce mai vizați. Este esențial să rămâneți vigilenți și la curent cu evoluțiile acestei escrocherii în viitor.

Această înșelătorie funcționează prin escroci care contactează persoane bogate și le prezintă oportunități de investiții profitabile. De obicei, escrocul, pretinzând că este un investitor experimentat în criptomonede, abordează persoane neavizate care afișează averi semnificative.

Diferite tipuri ale acestei înșelătorii

De obicei, există diferite tipuri de revendicări:

- **Taxe inițiale:** Escrocii ademenesc persoanele cu promisiunea unor randamente ridicate din investiții. Cu toate acestea, pentru a iniția procesul, aceștia impun un avans, de la 250 EUR la 1000 EUR (sau echivalentul în moneda națională în cauză), de obicei la capătul inferior al acestui interval. La primirea acestei plăți inițiale, escrocul dispare pur și simplu, lăsând victima cu mai puține finanțe și fără nicio investiție potențială.
- Într-o abordare mai complexă, procesul implică un apel video live, în timpul căruia escrocul prezintă un „cont financiar” care pretinde că aparține viitoarei victime care se confruntă cu un influx substanțial de bani. În timp ce aceste conturi sunt concepute pentru a părea legitime, ele sunt de fapt copii de design și nu au nicio legătură cu instituțiile financiare tradiționale.
- Uneori, victimele primesc o „primă plată”, de exemplu, între 50 EUR și 100 de EUR, pe care escrocii o prezintă drept dobândă la investițiile realizate – scopul este de a le determina să investească sume mai mari ulterior.
- Furtul de identitate: Pentru a crea o iluzie a legitimității, escrocii ar putea să solicite detalii personale de identificare ale victimei, pretinzând că sunt necesare pentru transferuri de fonduri sau anumite depuneri. Cu toate acestea, în loc să ajute la o investiție reală, ei obțin accesul neautorizat la datele personale și financiare ale victimei. Victimele uită să-și blocheze documentele de identitate la instituția financiară sau chiar trimit copii ale acestor informații escrocului.

Cum se soluționează această problemă

- **Nu efectuați transferuri suplimentare.** Adesea, escrocii menționează costuri mici de transfer sau costuri de plată care par foarte mici în comparație cu suma totală a înșelătoriei. Exemplu: o taxă de 600 EUR pentru o escrocherie de 60.000 EUR.
- **Victima nu trebuie să întrerupă contactul.** De obicei, în momentul în care victima se adresează unui organ de aplicare a legii, contactul ei cu escrocul a fost deja întrerupt. Dacă nu este cazul, menținerea contactului

Pentru utilizatorii care au mai puțină experiență în investiții, finanțe sau în utilizarea instrumentelor online, escrocii instalează adesea software de acces de la distanță.

Acest software este conceput în primul rând pentru acces, control și asistență de la distanță. Permite utilizatorilor să acceseze de la distanță și să controleze desktopul sau laptopul și serverele din orice colț al lumii. Victima instalează adesea un astfel de software cu ajutorul unui escroc. Odată ce conexiunea a fost stabilită, victimele uită adesea să dezinstaleze software-ul. Urmele lăsate de acest software pot constitui probe valoroase pentru investigațiile organelor de aplicare a legii, dacă sunt protejate și păstrate în mod corespunzător.

În funcție de tipul de software utilizat, există diferite tipuri de caracteristici, inclusiv:

- **Control la distanță:** Utilizatorii pot controla un computer dintr-o altă locație, ca și cum s-ar afla chiar lângă acesta. Acest lucru este util pentru depanarea problemelor, oferirea de suport la distanță sau accesarea fișierelor.
- **Transfer de fișiere:** Software care permite utilizatorilor să transfere fișiere între computere. Acest lucru duce uneori la instalarea unui „keylogger", un tip de soft de spionaj care monitorizează tot ceea ce tastează utilizatorul, și poate partaja informații cu escrocii ani de zile după ce a fost instalat pe un computer.
- **Acces de la distanță:** Acest lucru permite escrocilor să acceseze computerul sau serverul victimei de la distanță și să modifice fișiere, să instaleze programe sau să inițieze conexiuni.
- **Acces mobil:** Acest lucru permite controlul de la distanță al dispozitivelor cu ajutorul unui smartphone sau al unei tablete.

ar putea ajuta investigația, permițând căutarea instrumentelor utilizate în comiterea infracțiunilor cibernetice.

- **Victimele nu ar trebui să dezinstaleze** niciun software care a fost instalat pe dispozitivele lor, deoarece acesta ar putea lăsa urme de securitate cibernetică utile pentru investigații. Cu toate acestea, victima ar trebui să fie conștientă de posibilitatea de a avea pe dispozitiv un software care urmărește ceea ce tastează sau care menține camera pornită etc. Dacă acesta este cazul, victima ar trebui să-și limiteze utilizarea dispozitivului.
- **Examinați ce informații personale au fost publicate.** Dacă este posibil, schimbați datele de conectare la bănci și cereți parole noi pentru instrumentele de identificare electronică, dacă sunt utilizate astfel de instrumente.
- **Vedeți secțiunea despre înșelătorii secundare** mai sus la p. 38.
- **Măsurile adecvate care trebuie luate depind de specificul situației în care a ajuns victima.** Pentru mai multe detalii, vedeți secțiunea „Cele mai bune practici pentru fiecare tip de tranzacție", p. 24.

O altă variantă a acestei înșelătorii este utilizarea aparentei susțineri a celebrităților false. Escrocii își însușesc în mod abuziv fotografii reale și le combină cu conturi fabricate sau materiale promoționale, făcând să pară că personalități renumite garantează escrocheria.

Extorcare și șantaj sexual

În cazurile de extorcare, persoanele primesc adesea un e-mail sofisticat care le informează în mod fals că un hacker a obținut acces la computerul lor și se poate conecta la camera unui laptop sau a unui smartphone. Când vine vorba de șantaj sexual (sextortion) hackerul pretinde a filmat victima în timpul unui act de masturbare.

Ce reprezintă?

Persoana primește un e-mail de la un escroc. Acest e-mail spune că escrocul a spart computerul sau smartphone-ul victimei și a obținut acces la cameră. În cazurile de șantaj sexual, escrocul susține apoi că a înregistrat imagini cu victima în timpul unui act de masturbare și va publica acel videoclip dacă victima nu îl plătește în criptomonede.

Victima este instruită să transfere fonduri într-un anumit portofel de criptomonede într-un termen scurt pentru a preveni distribuirea unor astfel de presupuse imagini către contacte de afaceri și private, despre care hackerul susține că le-ar fi găsit pe dispozitiv. Ca „dovadă" a afirmațiilor sale, hackerul oferă de obicei o listă de nume de utilizatori și parole asociate cu diverse site-uri web, sugerând că victima a folosit acreditări identice pe mai multe site-uri de conținut pentru adulți.

Un mesaj e-mail original trimis autorului acestei publicații:

Subiect: Te-am înregistrat - (aici escrocul transmite parola care a fost găsită în breșă)
Data: 2023-06-22 3:32
Expeditor: „Salvează-ți viața” <xxxxxxxxxf@xxxx.ga>
Destinatar: XXXXXX@xxxx.com

Bună, sunt hacker și programator, știu că una dintre parolele tale este: (parola utilizatorului extrasă din scurgeri de parole)

Computerul tău a fost infectat cu malware-ul meu privat, deoarece browserul tău nu a fost actualizat/patch-uit, în acest caz este suficient doar să vizitezi un site web unde este plasat iframe-ul meu pentru a fi infectat automat dacă vrei să afli mai multe – caută pe Google: „Drive-by exploit”.

Malware-ul meu mi-a oferit acces complet la toate conturile tale (vezi parola de mai sus), control deplin asupra computerului tău și mi-a fost posibil să te spionez prin camera web.

Am colectat toate datele tale private, am înregistrat câteva videoclipuri cu tine (prin intermediul camerei web) și te-am ÎNREGISTRAT ÎN MOMENTE DE AUTOSATISFACȚIE!!

Pot publica toate datele tale private oriunde, inclusiv pe darknet, unde sunt oameni foarte bolnavi, și videoclipurile cu tine să le trimit contactelor tale și să le postez pe rețelele de socializare și oriunde altundeva!

Numai tu mă poți împiedica să fac asta și numai eu te pot ajuta. Nu au mai rămas urme, deoarece am șters malware-ul după ce mi-am terminat treaba și acest e-mail a fost trimis de pe un server piratat...

Singura modalitate de a mă opri este să plătești exact 400$ în Bitcoin (BTC).
Este o ofertă foarte bună, în comparație cu toate căcaturile acelea ORIBILE care se vor întâmpla dacă nu plătești!
Poți cumpăra cu ușurință Bitcoin aici: www.xxxxxxx.com, www.xxxxx.com, www.xxxxxx.com sau caută un bancomat Bitcoin în apropiere sau caută pe Google alte schimburi de criptomonede.
Poți trimite Bitcoin direct în portofelul meu sau crea propriul portofel mai întâi aici: www.login.xxxxx.com/en/#/signup/, apoi le primești și le trimiți mie.
Portofelul meu Bitcoin este: **17yshaYmvdp4yjU3WoCwowh6HHjTfEGDuG**
Copiază-l și lipește-l; este (cAsE sEnSEtiVE). Ai 3 zile.

Deorece am acces la acest cont de e-mail, voi ști dacă acest e-mail a fost citit.

Dacă primești acest e-mail de mai multe ori, este pentru a asigura că îl citești, agentul meu de corespondență este configurat astfel, iar după ce efectuezi plata, îl poți ignora.

După primirea plății, îți șterg toate datele și îți poți trăi viața în liniște ca înainte. Data viitoare, actualizează-ți browserul înainte de a naviga pe net!

Nina-Louise Siedler, în Riga, conduce un atelier pentru factorii de decizie din cinci state participante, împărtășind informații de la mesele rotunde virtuale de reglementare a activelor. Sesiunea s-a axat pe legislația paneuropeană referitoare la activele virtuale, cu scopul de a identifica deficiențele de reglementare și de a evidenția noi evoluții relevante pentru statele participante.

Cum se soluționează această problemă

Cele mai bune practici în sprijinirea victimelor care raportează e-mailuri de extorcare.

- **Rămâneți calm:** Dacă utilizatorul a primit un e-mail de șantaj sexual, este nevoie să rămână calm. Exemplul e-mailului prezentat mai sus arată că infractorii folosesc adjective puternice cu scopul de a insufla frică, de a crea senzația de urgență și de a induce rușine și panică.

- **Victima nu trebuie să interacționeze** cu expeditorul în niciun fel: E-mailurile de șantaj sexual de obicei nu trimit nimic ca dovadă și nu conțin atașamente. Dacă există link-uri trimise împreună cu e-mailul, utilizatorul nu trebuie să le deschidă.

- Utilizatorului trebuie să i se interzică să schimbe FIAT în criptomonede și să le transfere într-un portofel suspect de criptomonede.

- **Verificați portofelul de criptomonede:** O modalitate de a evalua autenticitatea unei adrese de portofel de criptomonede este prin intermediul instrumentelor denumite, de obicei, „exploratori de portofele". De exemplu, portofelul de criptomonede menționat poate fi examinat folosind următorul link:

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

- La o investigație inițială, care rămâne gratuită și durează mai puțin de 10 secunde, este deja evident că acest portofel a înregistrat mai multe tranzacții. Acest lucru contrazice adesea afirmația hackerului că ar fi o adresă de portofel cripto care este unică și utilizată o singură dată. Tranzacțiile multiple sugerează că mai multe persoane ar fi transferat fonduri către acesta.

- **Utilizarea pieței de conturi furate în avantajul victimelor:** Victimele pot folosi servicii gratuite precum: https://haveibeenpwned.com, care le permit să verifice dacă au avut loc breșe în datele lor prin analizarea miliardelor de scurgeri ale detaliilor de conturi. Introducând adresa de e-mail sau numele de utilizator, utilizatorii pot vedea dacă informațiile lor apar în breșe cunoscute. Dacă atacatorul prezintă o parolă care este utilizată, schimbați-o imediat pe toate platformele pe care este utilizată.

Atunci când se investighează persoane suspectate de extorcare, este esențial să se urmărească plățile până la portofelele lor de criptomonede.

În acest fel, se poate vedea dacă vreunul dintre portofele este legat de platformele financiare oficiale, ceea ce poate ajuta organele de aplicare a legii să identifice persoanele ce au trimis bani suspectului. Deși plata către un portofel de extorcare nu este o infracțiune, cei care au făcut-o ar putea deține informații relevante sau s-ar putea confrunta cu amenințări similare din partea aceleiași persoane, ceea ce poate ajuta investigația.

Cursuri de formare găzduite de Secretariatul OSCE din Viena, organizate pentru factorii de decizie ucraineni cu privire la lacunele de reglementare în domeniul activelor virtuale, cu accent pe schimburile descentralizate.

Înșelătorii de tip “Rug Pull”

Escrocherii de tip „ieșire”, escrocherii pump-and-dump sau escrocherii „rug pull” (denumire provenită din expresia, „a trage prețul sub picioare”) sunt scheme în care escrocii creează mult entuziasm în jurul unui nou activ digital. Poate fi orice tip de activ digital, nu doar o nouă criptomonedă. Astfel de înșelătorii au fost făcute și cu proiecte și jetoane nefungibile (NFT). Escrocii ies apoi rapid din proiect, furând banii investitorilor și lăsând activul digital fără valoare.

Ce reprezintă?

Obiectivul acestui tip de înșelătorie este de a atrage cât mai mulți cumpărători sau investitori pentru noul activ digital și să umfle artificial, cât mai mult posibil, valoarea percepută a acestuia. Odată ce escrocii au strâns suficienți bani, dispar (aici intervine partea de „exit” din exit scam, sau înșelătoria cu ieșire) și păstrează banii. Această ieșire se poate întâmpla rapid, când toți cei implicați dispar fără urmă, sau treptat prin retragerea lentă a fondurilor și reducerea dezvoltării proiectului. În cazul din urmă, uneori poate fi greu de distins între o adevărată fraudă de tip „rug pull” și un proiect eșuat, dar lansat cu bune intenții.

În ambele cazuri, ieșirea escrocilor înseamnă că activul se dovedește a fi fals și devine fără valoare. Victimele rămân fie cu mai multe monede sau jetoane care valorează o fracțiune din cât au plătit pentru ele, dacă pot găsi un cumpărător, fie activul digital conține un cod care indică faptul că activul nu poate fi vândut deloc.

Înșelătorii de tip phishing

Escrocheriile de tip phishing sunt o înșelătorie comună în multe domenii ale internetului. Este, de asemenea, o înșelătorie comună și eficientă legată de activele digitale.

Ce reprezintă?

Escrocii pretind că reprezintă o afacere oficială, având site-uri web sau acte corporative cu aspect legitim, și trimit mii de e-mailuri și mesaje cu link-uri ce duc la versiunea falsă a unui site web. Acest site web este creat pentru a permite conectarea și stocarea informațiilor personale ale fiecărui vizitator, precum și toate adresele și parolele cripto (numite „chei de portofel cripto”) pe care aceștia le introduc. Acest lucru este deosebit de important în cazul infracțiunilor cripto, deoarece, spre deosebire de alte tipuri de conturi, dacă cheia privată a unui portofel cripto este furată, atunci contul este aproape imposibil de recuperat. Aceasta înseamnă că fondurile din portofel sunt pierdute pentru totdeauna.

Diferite tipuri ale acestei înșelătorii

Potrivit unui raport publicat de un furnizor de analiză blockchain,[17] noi tipuri de înșelătorii precum phishing implică stârnirea sentimentului „FOMO” (teama resimțită de indivizi că ar putea rata oportunități) în noii investitori cripto, determinând victimele să trimită bani în contul greșit în speranța de a cumpăra un NFT. Aceasta înseamnă că victimele pierd doar suma de bani pe care au trimis-o în contul greșit, nu întregul portofel.

17 Illicit Crypto Ecosystem Report. (2023) /Raport privind ecosistemul cripto ilicit. (2023), disponibil la adresa: https://www.trmlabs.com/report (accesat: august 2023).

O altă variantă de înșelătorie, din ce în ce mai răspândită, este „address poisoning” („otrăvirea adresei”). În acest caz, escrocul creează o adresă care seamănă cu cea căreia victima vizată a trimis anterior fonduri. Apoi escrocul trimite o cantitate mică de criptomonede victimei, în speranța că aceasta va efectua, fără să vrea, o plată viitoare la adresa frauduloasă în locul destinatarului vizat inițial.

Ce se poate face pentru a o evita?

Ar trebui să fim conștienți de link-urile false de phishing și să verificăm toate linkurile.

Verificați de două ori adresele:

- Verificați întotdeauna adresa la care trimiteți fonduri, mai ales atunci când tranzacționați sume mari. Nu mizați doar pe funcțiile clipboard-ului, adică a unei zone de memorie, unde conținutul este stocat temporar (așa-numita funcție copy-paste), deoarece malware-ul le poate manipula pentru a lipi adresa portofelului de criptomonede, diferită de cea pe care victima credea că a copiat-o.

- Utilizați marcaje pentru site-urile cripto vizitate frecvent. Astfel veți evita riscul de a tasta greșit sau de a ateriza pe un site de phishing care arată similar.

Activați măsuri de securitate suplimentare:

- Se recomandă utilizarea autentificării cu doi factori (2FA) de câte ori este posibil. Acest lucru adaugă un nivel suplimentar de securitate, ceea ce face mai dificilă accesarea conturilor de către escroci.

- Actualizați și puneți în aplicare în mod regulat software anti-malware pentru a detecta și elimina potențialele amenințări de pe dispozitivul dvs. Unele tipuri de malware sunt concepute pentru a monitoriza tranzacțiile cripto sau pentru a modifica datele clipboard-ului.

Utilizați manageri de parole: Managerii de parole sunt instrumente software concepute pentru a stoca, gestiona și completa automat parolele. De asemenea, acestea permit utilizatorilor să creeze note sigure ce pot salva în siguranță numerele portofelelor de criptomonede pentru diferite conturi online.

Atacuri de tip man-in-the-middle („omul de la mijloc”)

Ce reprezintă?

În acest tip de înșelătorie, escrocii nu vizează direct o victimă, ci interceptează transmiterea datelor atunci când persoana își accesează contul de criptomonede pe o rețea WiFi publică sau nesecurizată, adică locurile unde site-urile web vizitate și informațiile trimise de la computer la site nu sunt private. Escrocii colectează adresa portofelului cripto, detaliile de conectare și cheile portofelului și apoi le utilizează pentru a prelua contul.

Cum le abordăm sau le evităm?

Acest tip de înșelătorie poate fi evitat prin utilizarea unei rețele private virtuale (VPN). Acestea sunt destul de ieftine, de obicei doar 3 - 4 EUR pe lună. VPN-urile criptează conexiunea utilizatorului la internet, astfel încât persoanelor neautorizate le va fi mai dificil să vizioneze ce site-uri web sunt vizitate sau ce este tastat. De asemenea, această metodă ascunde adresa IP originală a utilizatorului, permițând navigarea anonimă și împiedicând vizibilitatea locației geografice reale a utilizatorului. Acest lucru permite utilizatorilor să aibă acces de la distanță la resursele organizației lor sau să evite cenzura.
(Vedeți mai multe informații în secțiunea „Colectarea adreselor IP”, p. 31.)

Site-uri web false care imită schimburile de criptomonede

Ce reprezintă?

În loc să creeze o criptomonedă falsă, escrocul creează site-uri web care arată ca platforme de tranzacționare pentru criptomonede. Când victima accesează acest site pentru a-și schimba tipul de criptomonedă într-un alt tip sau în monedă FIAT, escrocii îi fură atât detaliile personale, cât și criptomoneda depusă.

Cum le abordăm sau le evităm?

Pentru a spori securitatea, utilizați întotdeauna autentificarea cu doi factori (2FA) atunci când vă conectați la platforma de schimb pe care o utilizați. Acest nivel suplimentar de verificare poate implica primirea unui cod unic prin SMS sau e-mail, pe care trebuie să-l introduceți în timpul procesului de conectare. Alternativ, dacă statul participant la OSCE oferă o soluție de identificare electronică, luați în considerare utilizarea acesteia ca o măsură suplimentară de protecție în timpul conectării.

Înșelătorii secundare

Există, de asemenea, înșelătorii secundare care apar după ce o victimă a fost înșelată anterior. Acestea sunt acoperite în secțiunea „Sprijin pentru victime”, p. 37.

De la stânga la dreapta: Marcin Zarakowski, Michal Gromek, Anna Pajewska și Nina-Louise Siedler, care au condus un atelier independent, axat pe provocările și avantajele supervizării furnizorilor de servicii de active virtuale (VASP) pentru delegația ucraineană. Sesiunea a inclus reprezentanți ai instituțiilor ucrainene cheie, cum ar fi Banca Națională a Ucrainei, Serviciul de Monitorizare Financiară de Stat al Ucrainei, Ministerul pentru Transformare Digitală și Comisia Națională pentru Valori Mobiliare și Burse. Atelierul a fost găzduit cu generozitate de Ministerul Polonez de Finanțe, care continuă să-și ofere spațiile gratuit pentru o serie de sesiuni de instruire pentru delegații ucraineni.

Instrumente suplimentare pentru investigarea infracțiunilor legate de activele virtuale

Instrumente suplimentare pentru investigarea infracțiunilor legate de activele virtuale

Instrumente de analiză blockchain

Un instrument bun de analiză blockchain sau un explorator de portofele (wallet explorer) le permite polițiștilor să desfășoare o parte din investigații fără a fi nevoiți să mizeze pe informațiile de la VASP, care pot fi furnizate lent sau incomplet. În plus, încă nu toate VASP-urile utilizează instrumente de analiză blockchain.

De ce contează acest lucru:

Organele de aplicare a legii solicită frecvent informații de la VASP-uri despre soldul actual de pe anumite adrese de portofel de criptomonede. În timp ce unitățile de conformitate VASP sunt dotate pentru a răspunde la aceste interpelări, solicitările de acest fel sunt asociate cu un volum semnificativ de lucru din punct de vedere administrativ. O alternativă mai eficientă este introducerea adresei portofelului de criptomonede într-unexplorator de portofele, care oferă apoi rapid informațiile necesare pentru majoritatea criptomonedelor de top, însă nu pentru toate.

Informații oferite de instrumentele de vizualizare (exploratorii de portofele):

- Soldul curent în criptomonede și principalele monede FIAT, de ex.
- USD Total fonduri primite în portofelul de criptomonede.
- Total fonduri trimise din portofelul de criptomonede.
- Marcaje temporale pentru tranzacții. (Notă: orele tranzacțiilor pot varia în funcție de fusul orar).
- Taxe suportate pe blockchain.
- Adresele portofelelor-sursă de criptomonede (de unde au fost transferate fondurile).
- Adresele portofelelor-destinație de criptomonede (unde au fost trimise fondurile).

Pentru cei care nu sunt familiarizați cu analiza blockchain, aceste date ar putea părea superficiale. Cu toate acestea, în scopuri de investigație, ele pot oferi informații valoroase, cum ar fi afișarea unui tipar cu multe tranzacții mici de intrare, împreună cu mai puține tranzacții mari de ieșire. Acest tip de comportament ar putea sugera activități asemănătoare cu cele ale unui traficant de droguri.

Exemple din lumea reală:

S-a constatat că următoarele portofele au fost implicate în cazuri penale:

- Portofelul de criptomonede legat de un caz de șantaj sexual: Blockchain Explorer
- Portofel de criptomonede asociat cu Twitter Hack, un explorator de portofele ce colectează informații de la utilizatori și Chain Abuse

La fel ca și în cazul tuturor informațiilor cu sursa deschisă (open source), orice date obținute de la astfel de exploratori ar trebui abordate cu scepticism și verificate înainte de a trage concluzii.

Exemple de instrumente gratuite de analiză blockchain:

- Block Explorer: Acesta este un instrument simplu care oferă informații detaliate despre blocurile, adresele și tranzacțiile Bitcoin. Este un bun punct de plecare pentru începători.
- Etherscan: Acest instrument este special pentru blockchain-ul Ethereum și poate oferi analize detaliate ale tranzacțiilor și adreselor.
- Blockchair: Acest instrument versatil acoperă mai multe blockchain-uri, de la Bitcoin la Ethereum, fiind versatil pentru cei care doresc să analizeze diferite rețele.

Olga de Truchis și Greta Barkauskienė, experte OSCE în active virtuale și Co-Coordonatoare ale Programului Europol „Parteneriat public-privat pentru Informații Financiare cu privire la Criptoactive (EFIPPP), au participat la plenara EFIPPP organizată în aprilie 2024 la sediul Europol din Haga. Împreună, ele au facilitat sesiuni de schimb de cunoștințe, în cadrul cărora participanții din diferite țări, inclusiv țări beneficiare ale OSCE, au explorat și discutat despre acest modus operandi emergent al criminalității organizate în domeniul activelor virtuale.

Furnizori de instrumente analitice blockchain

Furnizorii de instrumente analitice blockchain sunt omologii comerciali ai exploratorilor de portofele.

Aceștia folosesc software specializat conceput pentru a monitoriza, analiza și vizualiza activitățile din rețelele blockchain. Aceste instrumente ajută investigatorii să descopere tipare, să urmărească tranzacțiile și să obțină informații despre vastul și complexul univers al blockchain-ului.

Dincolo de datele disponibile colectate cu ajutorul unui explorator de portofele, furnizorii de analiză blockchain oferă:

- **Urmărire și trasabilitate:** Majoritatea instrumentelor de analiză pot urmări și trasa parcursul unei tranzacții cu criptomonede de la sursă până la destinație. Acest lucru este vital pentru înțelegerea fluxului de fonduri și identificarea oricăror potențiale activități ilegale.
- **Vizualizare:** Aceste instrumente oferă adesea scheme vizuale și grafice pentru a facilita înțelegerea unor cantități mari de date dintr-o privire și pentru a conecta portofelele de criptomonede la instituții financiare sau pentru a lega tranzacțiile ori furnizorii de portofele între ei.
- **Evaluarea riscurilor:** Analizând tiparele de tranzacții, unele instrumente pot evalua riscul asociat cu anumite portofele sau tranzacții, oferind informații valoroase pentru instituțiile financiare și autoritățile de reglementare.
- **Date cuprinzătoare:** Aceste instrumente pot extrage și integra date din diferite blockchain-uri, oferind utilizatorilor o viziune de ansamblu asupra criptomonedelor, ceea ce poate fi util pentru un număr mai mare de investigații.
- **Servicii de demixare:** Unii furnizori susțin că serviciile lor sunt capabile să afișeze tranzacții prin mixere și tumbler-e, care sunt servicii concepute pentru a spori confidențialitatea și anonimatul tranzacțiilor cu criptomonede.
  (Vedeți secțiunea „Mixere și tumbler-e”, p. 19, precum și discuția despre serviciile de demixare din secțiunea „Trimiterea cazurilor în instanță”, p. 34, pentru mai multe informații.)

Utilizând aceste instrumente, cercetătorii pot înțelege mai bine dinamica complicată a universului blockchain, asigurând decizii informate și o percepție mai profundă a acestei tehnologii revoluționare.

Sediul central al Băncii Naționale a Georgiei: în ultimii doi ani, echipa de active virtuale a primit sprijin important din partea experților OSCE în active virtuale. Drept rezultat, scorul Georgiei în MONEYVAL a fost ridicat la „În mare parte conform" cu recomandarea 15 a GAFI.

Cooperarea cu experții în active digitale

Cooperarea cu experții în active digitale

Atunci când se gestionează active digitale și rapoartele aferente într-o unitate a organelor de aplicare a legii, colaborarea cu entități externe devine esențială. Aceste entități includ organizații internaționale de poliție, bănci și unități specializate din anumite țări. Expertiza lor contribuie la o gestionare eficientă a investigațiilor.

Identificarea competențelor locale

Este extrem de util să identificați angajați locali ai organelor aplicare a legii care au experiență în active virtuale. Datele lor de contact pot fi utile din următoarele motive:

- **Scop:** Să răspundă la întrebări dificile și să obțină informații valoroase în procesul de sesizare.
- **Exemplu:** Agenția Națională pentru Combaterea Criminalității (NCA) din Regatul Unit a creat o unitate dedicată criptomonedelor, care poate acționa ca o echipă de consultare pentru cazuri complicate. Mai multe idei pentru modul de organizare a cooperării în cadrul organelor de aplicare a legii în ceea ce privește activele virtuale puteți găsi și în Typologies Report 2023 / Raportul de tipologii 2023, întocmit de Consiliul Europei.[18]

Sprijin internațional

Platforma Europol pentru Experți (EPE)

- **Descriere:** Aceasta este o platformă gratuită pentru asistență practică în domeniul activelor virtuale, creată pentru angajații organelor de aplicare a legii.
- **Eligibilitate:** Pentru a fi eligibilă pentru accesarea EPE (https://epe.europol.europa.eu/), o țară trebuie să fie membră a Uniunii Europene sau să fie parte la așa-numit acord operațional.[19]
- **Avantaje:** EPE oferă cele mai bune practici privind investigațiile în domeniul activelor virtuale. De asemenea, platforma oferă acces la webinare și date de contact ale părților interesate, informații despre conferințe și alte resurse de învățare.
- **Procesul de aderare:** Dacă un stat participant la OSCE face parte din acordul operațional[20] (lista furnizată separat), acesta poate solicita accesul. Procedura de aderare implică următorii pași:
  - Contactarea autorității desemnate la o3 (at) europol.europa.eu folosind un e-mail de serviciu și specificați ce legătură aveți cu activele virtuale și modul în care cunoștințele dvs. vor aduce beneficii altora.
  - Specificarea clară a motivul aderării, în special în ceea ce privește activele virtuale.
- **Cine poate adera:** Deși platforma este concepută în primul rând pentru funcționarii organelor de aplicare a legii, experți din afara acestui cerc atât din sectorul public, cât și cel privat, pot, de asemenea, aplica. Cu toate acestea, complexitatea informațiilor accesibile ar putea fi limitată pentru profesioniștii din afara organelor de aplicare a legii.
- **Cost:** Nu se percepe nicio taxă. Accesul este complet gratuit.

În octombrie 2019, Europol a lansat două jocuri educaționale numite „Cryptopol". Acestea au fost actualizate de mai multe ori și includ mai multe criptomonede. Acestea rămân gratuite pentru organele de aplicare a legii din statele membre ale UE. Accesați prin: o3@europol.europa.eu.

18 Căutați 'Case Boxes' -Typologies Report 2023 - Money Laundering and Terrorist Financing Risks in the World of Virtual Assets, Moneyval, Council of Europe https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4 (accesat la 25 februarie 2024).

19 Acorduri și înțelegeri operaționale cu țări. Europol https://www.europol.europa.eu/partners-collaboration/agreements (accesat la 26 noiembrie 2023).

20 Acorduri și înțelegeri operaționale cu țări. Europol https://www.europol.europa.eu/partners-collaboration/agreements (accesat la 26 noiembrie 2023).

Centrul INTERPOL Anticorupție și Criminalitate Financiară (IFCACC)

Centrul INTERPOL Anticorupție și Criminalitate Financiară (IFCACC): Acesta este un centru dedicat combaterii infracțiunilor financiare transnaționale pentru a proteja sistemele financiare globale.

Eligibilitate: Abordând preocuparea crescândă în legătură cu globalizarea infracțiunilor financiare, INTERPOL a lansat Centrul IFCACC ca un răspuns consolidat pentru a ajuta la combaterea acestor provocări. Activitățile acestui Centru se extind dincolo de simpla aplicare a legii, fiind relevante și pentru organismele internaționale și părțile interesate.

Avantaje: IFCACC facilitează:

- Sprijin în caz de fraudă, infracțiuni de plată și anchete transfrontaliere din partea organelor de aplicare a legii.
- Asistență în combaterea spălării banilor, recuperarea activelor și înțelegerea activelor virtuale.
- Supravegherea practicilor anticorupție, de la preocupări legate de sport, la discrepanțe politice la nivel înalt.

Procesul de aderare: Dat fiind faptul că IFCACC operează bazându-se pe un model constituit din mai multe agenții, potențialele colaborări implică:

- Stabilirea contactelor cu Secretariatul General al INTERPOL sau cu Biroul Central Național al INTERPOL, care de obicei se află în subordinea ministerului de justiție și poliția judiciară a statului respectiv.
- Demonstrarea angajamentelor clare în legătură cu obiectivele împotriva infracțiunilor financiare și a corupției.
- Exprimarea potențialelor domenii de colaborare sau nevoi.

Cine poate adera: Pe lângă organele de aplicare a legii, instituțiile financiare, entitățile internaționale și reprezentanții sectorului privat pot interacționa cu IFCACC. Cu toate acestea, profunzimea colaborării poate varia în funcție de natura și scopul asocierii.

Cost: Dat fiind faptul că INTERPOL este o organizație internațională, nu există niciun cost asociat cu colaborarea cu Secretariatul General.

Pentru informații suplimentare despre IFCACC și I-GRIP, consultați:

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

Pentru informații suplimentare legate de aspectele tehnice ale activelor virtuale, angajații organelor de aplicare a legii pot trimite un e-mail la: innovation@interpol.int

Resursă suplimentară: angajații organelor de aplicare a legii pot solicita Ghid INTERPOL pentru confiscarea activelor virtuale: vaguidelines@interpol.int

Programe UNODC cu privire la active virtuale pentru combaterea criminalității informatice și a spălării banilor și ateliere de investigație

Prezentare generală: Condusă de echipa Oficiului Națiunilor Unite pentru Droguri și Criminalitate (UNODC), această serie cuprinzătoare de ateliere oferă o explorare aprofundată a activelor virtuale, a infracțiunilor financiare și a domeniului esențial al conformității.

Curriculum-ul este structurat în sesiuni de bază, avansate și în cascadă, definite ca formare de formatori, încurajând împărtășirea celor mai bune practici din industrie. Atelierele îmbină aspecte teoretice riguroase cu exerciții practice, echipând participanții din organele de aplicare a legii cu abilități neprețuite în urmărirea, investigarea și gestionarea eficientă a activelor virtuale.

Eligibilitate: Această formare specializată este organizată pentru profesioniști din diverse sectoare, cum ar fi aplicarea legii, instituții financiare, întreprinderi tehnologice și domenii educaționale. Este o resursă neprețuită pentru factorii de decizie politică, autoritățile de reglementare, ofițerii de investigație și toți profesioniștii interesați de decodificarea complexității activelor virtuale, dinamica blockchain și arta atenuării infracțiunilor financiare.

Domenii cheie de interes:

- **Elementele esențiale ale activelor virtuale:** Explorați în profunzime geneza, evoluția și aspectele complexe ale activelor virtuale în continuă schimbare și tehnologiile care stau la baza lor.
- **Dinamica tranzacțiilor:** Decodați ciclul de viață al tranzacțiilor blockchain, de la început până la finalizare.
- **Blockchain în profunzime:** Descoperiți procesele prin care sunt înregistrate, ratificate și arhivate tranzacțiile pe blockchain.
- **Criminalistica blockchain:** Deveniți competenți în supravegherea tranzacțiilor în timp real și discerneți tiparele folosite de răufăcători pentru a-și ascunde identitățile.
- **Tactici CSB/CFT:** Învățați să calibrați protocoalele de combatere a spălării banilor și a finanțării terorismului pentru a vă alinia la peisajul metamorfic al activelor virtuale.
- **Gestionarea riscurilor:** Cu scopul de a familiariza participanții cu standardele de aur (golden standards) în atenuarea riscurilor distincte legate de activele virtuale.
- **Supravegherea activelor:** Cu scopul de a le oferi participanților cele mai bune practici în arta confiscării și administrării adecvate a activelor virtuale în timpul investigațiilor.

Procedura de înscriere: Potențialii participanți pot:

- Consulta calendarul viitoarelor ateliere și își pot asigura locurile.
- Stabili potențialele reduceri de taxe, reieșind din experiența lor profesională prin intermediul formularului specificat.
- Citi cu atenție și accepta termenii expliciți de participare în instruiri.

Public țintă:
Atelierele sunt concepute pentru a rezona cu un public divers, cuprinzând investigatori, cei pasionați de drept, reprezentanții autorităților de reglementare financiară, pionieri în tehnologie, jurnaliști și alții. Acestea sunt utile atât sectorului public, cât și celui privat, adresându-se celor pasionați de activele virtuale și de normele fiscale corelate.

Structura taxelor: Estimările pentru costul unei sesiuni de instruire variază de la 10.000 USD până la 20.000 USD, în funcție de numărul de participanți. Prețurile preferențiale sunt potențial accesibile pentru delegații din sectorul public, academicieni, entități non-profit și lucrătorii din domeniul media. Informații suplimentare despre domeniul de aplicare al instruirii pot fi solicitate contactând Direcția de Instruire în domeniul activelor virtuale a UNODC prin e-mail: cryptocurrency@unodc.org

Caracteristici suplimentare:
Platforma de e-learning a UNODC poate fi accesată prin următorul link: https://www.unodc.org/elearning/en/courses/course-catalogue.html

Institutul Basel pentru Guvernanță

Institutul Basel pentru Guvernanță: Aceasta este o organizație independentă, non-profit, axată pe îmbunătățirea guvernanței și combaterea infracțiunilor financiare la nivel global. Cu sediul în Basel, Elveția, Institutul operează, de asemenea, în diferite țări africane, colaborând îndeaproape cu Universitatea din Basel.

Atelierul de criptomonede al Institutului Basel: Oferă un curs virtual cuprinzător de 4 zile, axat pe fundamentele criptomonedelor, criminalității financiare și conformității cu normele de prevenire a spălării banilor (CSB). Cursul cuprinde un scenariu practic de spălare a banilor, ghidând participanții să urmărească tranzacțiile blockchain pentru activități ilicite.

Eligibilitate: Este deschis unui spectru larg de profesioniști din organele de aplicare a legii, sectoare financiare, întreprinderi și chiar și studenți. Conținutul este adaptat pentru factorii de decizie politică, autoritățile de reglementare, jurnaliștii de investigație și oricine este interesat de activele virtuale, tehnologia blockchain și atenuarea infracțiunilor financiare.

Avantaje: Atelierul Institutului Basel oferă informații despre:

- **Fundamentele criptomonedelor:** Înțelegerea principiilor de bază, apariției și domeniului activelor virtuale, tehnologiei registrelor distribuite și multe altele.
- **Mecanica tranzacțiilor:** Înțelegerea modului în care funcționează rețeaua Bitcoin, criptografia și gestionarea tranzacțiilor.
- **Blockchain și minare:** Studierea modului în care tranzacțiile sunt securizate, stocate și validate în blockchain.
- **Analiza blockchain:** Tehnici de monitorizare a tranzacțiilor în timp real, eludarea anonimatului de către infractori și utilizarea instrumentelor.
- **Diligență necesară:** Adaptarea programelor CSB/CFT la noile metode de plată.
- **Managementul riscurilor:** Cele mai bune practici și surse pentru gestionarea riscurilor asociate activelor virtuale.
- **Confiscarea activelor:** proceduri și elemente specifice ce țin de confiscarea criptoactivelor, gestionarea portofelelor și multe altele.

Cine poate participa: Cursul este destinat investigatorilor, avocaților, profesioniștilor CSB/CFT, colaboratorilor unităților de informații financiare, practicienilor din domeniul FinTech, jurnaliștilor și multor altora. Este menit atât pentru profesioniștii din sectorul public, cât și cei din sectorul privat, interesați să navigheze în lumea activelor virtuale și a infracțiunilor financiare.

Cost: 750 CHF de persoană cu o reducere la de 300 CHF pentru anumiți membri, cum ar fi cei din sectorul public, academicieni, organizații non-profit și jurnaliști.

Pentru mai multe informații: info@baselgovernance.org

Detaliile cursului și link-urile de înregistrare pentru datele disponibile pot fi găsite pe platformele de socializare ale Institutului Basel.

Fundația FinCrime Fighters

Fundația FinCrime Fighters („Luptătorii împotriva infracțiunilor financiare") este o fundație cu sediul la Stockholm, creată de experți din Grupul Operativ pentru Active Digitale al Coaliției Globale pentru Combaterea Criminalității Financiare. Scopul acestui instrument este de a primi răspunsuri rapide și susținute de referințe la probleme legate de finanțe bazate pe blockchain și Web 3.

Fundația oferă un fond de jetoane gratuit pentru AI Assistant generativ, dedicat exclusiv celor care luptă împotriva criminalității financiare publice și private. Echipa publică și analizează în mod constant cele mai noi rapoarte, inclusiv materialele OSCE publicate. Reglementările pot fi căutate cu un sistem asemănător Chat GPT ce ajută practicienii să fie la curent cu modificările normative zilnic.

https://www.fincrimefighters.com/

Recomandări pentru organele de aplicare a legii după sesizare

Recomandări pentru organele de aplicare a legii după sesizare

- **Oferiți sprijin imediat:** asigurați-vă că victimele primesc îndrumări imediate cu privire la modul prin care pot securiza activele digitale rămase și la reducerea riscului de pierderi financiare suplimentare. Aceasta poate include sfaturi privind schimbarea parolelor, securizarea portofelelor sau transferul activelor către o platformă mai sigură.
- **Consiliere financiară:** Puneți victimele în legătură cu serviciile de consiliere financiară care le pot ajutasă înțeleagă pierderile suferite, potențialele implicații fiscale și strategiile derecuperare sau atenuare a pierderilor în timp.
- **Educați:** Lansați campanii și ateliere de conștientizare publică despre astfel de escrocherii. Cu cât publicul este mai informat, cu atât devine mai greu pentru escroci să înșele potențialii investitori.
- **Colaborați cu platformele de schimb:** Lucrați îndeaproape cu platformele de schimb de criptomonede pentru a urmări și, eventual, a îngheța activele escrocilor, îngreunându-le încasarea câștigurilor obținute ilegal.
- **Colaborare inter-jurisdicțională:** Deoarece înșelătoriile digitale depășesc adesea granițele, colaborați cu organele internaționale de aplicare a legii pentru a trasa, reține și asigura urmărirea penală a vinovaților.

Mariam Grigalashvili împărtășește informații din Georgia și Banca Națională a Georgiei cu colegii de la Banca Centrală a Armeniei din Erevan în timpul unui atelier axat pe impozitarea criptomonedelor și relația acesteia cu politicile CSB și CFT.

Rezumat și principii de cooperare cu OSCE

Rezumat și principii de cooperare cu OSCE

Inițiativa OSCE de sprijin în domeniul activelor virtuale

Cine suntem

Echipa de experți în active virtuale a OSCE este pregătită în mod unic pentru a răspunde provocărilor în continuă evoluție prezentate de activele virtuale pentru factorii de decizie și organele de aplicare a legii. Bazându-ne pe aproape cincizeci de ani de excelență în oferirea expertizei tehnice, ajutăm instituțiile politice și organele de aplicare a legii să navigheze în complexitatea activelor virtuale din cele 57 de state participante la OSCE.

Valoarea pe care o creăm pentru organele de aplicare a legii și pentru factorii de decizie

- **Cunoștințe de ultimă oră:** Instruirea noastră echipează organele de aplicare a legii și factorii de decizie cu informații și strategii actualizate, adaptate pentru a aborda provocările unice din domeniul activelor virtuale.
- **Eficiență operațională:** Oferim cursuri de instruire practică, asigurăm logistica, rezervăm locații, invităm experți verificați în active virtuale din statele participante la OSCE, propunem agendă și stabilim obiectivele de învățare.
- **Formare și dezvoltare a cunoștințelor:** Oferim programe cuprinzătoare de formare în domeniul activelor virtuale. Echipa noastră, care este formată din factori de decizie politică, organe de aplicare a legii, membri ai echipelor de conformitate ale băncilor tradiționale și companii WEB3, acordă prioritate învățării practice, cu o componentă teoretică scurtă și clară. Accentul principal este pus pe exerciții practice, ceea ce asigură aplicabilitatea în lumea reală. Participanții din trecut au văzut rezultate directe, inclusiv investigarea cu succes a cazurilor complexe de spălare de bani.
- **Furnizarea de resurse:** Colaborăm cu experți de top în blockchain. Această experiență practică în aplicarea instrumentelor profesionale le oferă membrilor posibilitatea de a utiliza în mod eficient cunoștințele însușite la sesiuni și ateliere de aprofundare, în procesul cărora transpunem procese complexe în exerciții.
- **Analiza de caz:** Cursul nostru include adesea studii de caz în timp real și suport legislativ, care reflectă evoluțiile în curs, și astfel ne asigurăm că vom putea rezolva provocările înainte ca acestea să se întâmple cu adevărat.
- **Scalabilitate și continuitate:** Sistemul nostru de formare în cascadă include un model de „instruire a formatorilor”, prin intermediul căruia echipăm experții cu capacitatea de a disemina aceste cunoștințe în continuare în propria jurisdicție. Acest lucru asigură o acoperire mai largă și o continuitate în dezvoltarea cunoștințelor speciale în țările de origine.
- **Construirea unui mediu digital mai sigur:** Asigurându-ne că factorii de decizie politică și organele de aplicare a legii sunt bine echipate pentru a face față problemelor ce țin de activele virtuale, contribuim în mod semnificativ la crearea unui mediu financiar digital mai sigur și mai transparent.

Alăturați-vă nouă pentru a modela viitorul securității cibernetice și pentru a asigura un domeniu digital mai sigur și mai transparent pentru toți.

Contactați-ne la:
VirtualAssets@osce.org

O scurtă selecție de lecturi suplimentare

O scurtă selecție de lecturi suplimentare

Oficiul Națiunilor Unite pentru Droguri și Criminalitate (UNODC)

Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies (2014) / Manual de bază privind detectarea și investigarea spălării produselor infracționale prin utilizarea monedelor virtuale (2014)

Deși a fost publicat de UNODC acum mai bine de zece ani, în 2014, acest document cuprinzător de 200 de pagini analizează în profunzime diverși termeni și oferă contextul pentru termenii descriși în această analiză. De asemenea, acesta conține chestionare detaliate de autoevaluare:

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

Organizația pentru Securitate și Cooperare în Europa (OSCE)

Handbook for Dealing with Virtual Currencies in Criminal Proceedings (2022) / Manual pentru gestionarea monedelor virtuale în cadrul procedurilor penale (2022)

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

Departamentul de Justiție al SUA

The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets (2022) / Rolul organelor de aplicare a legii în detectarea, investigarea și urmărirea activităților criminale ce țin de active digitale (2022)

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

Publicat de Departamentul de Justiție al SUA, raportul servește drept document complementar la Raportul cu privire la cooperare internațională dintre organele de aplicare a legii și actualizează Cadrul normativ în domeniul criptomonedelor. Oferă o imagine de ansamblu pentru referințe viitoare.

Despre autor

Această analiză a fost creată de Michal Gromek, un expert de top în active virtuale în cadrul proiectului OSCE ce vizează atenuarea riscurilor de spălare a banilor asociate activelor virtuale și criptomonedelor, implementat de către Biroul Coordonatorului Activităților Economice și de Mediu al OSCE (OCEEA). Domnul Gromek este un fost director de conformitate al VASP Safello cu sediul în Stockholm, tranzacționat la Nasdaq. Prezidează Grupul Operativ pentru Active Digitale din cadrul Coaliției Globale pentru Combaterea Criminalității Financiare, o colaborare stabilită între Europol, Forumul Economic Mondial și London Stock Exchange Risk Solutions (Servicii de administrare a riscurilor oferite de Bursa de valori din Londra). Gromek este, de asemenea, membru al echipei executive a Coaliției Globale pentru Combaterea Criminalității Financiare. El continuă să conducă sesiuni de instruire pentru guverne și organe de aplicare a legii, oferind sprijin în elaborarea legislației pentru a preveni provocările cu care se confruntă statele participante la OSCE. Și-a acumulat cunoștințele speciale prin rolurile anterioare în calitate de director executiv FinTech și de director de program al Diviziei de Educație Executivă de la Școala Economică de la Stockholm. Mai bine de zece ani a lucrat în domeniul conformității pentru Fintech și active virtuale. Constatările sale au fost publicate pe Forbes.com, precum și în diverse cărți și reviste.

Mulțumiri

Revizia și sugestiile făcute de dr. Alexandra Andhov au contribuit semnificativ la îmbunătățirea acestui ghid. Acuratețea, relevanța și profunzimea conținutului prezentat au sporit foarte mult datorită cunoștințelor și viziunilor ei din domeniul juridic. Prin prisma experienței sale ca profesor asociat la Facultatea de Drept a Universității din Copenhaga, ne-a oferit evaluări și recomandări neprețuite în scrierea acestui document. Dr. Andhov are experiență atât în drept, cât și tehnologie, contribuind la un număr semnificativ de proiecte în acest domeniu, în special în calitatea sa de co-fondator și director juridic al organizației Financial Crime Fighters.

Pentru a asigura cea mai înaltă lizibilitate și calitate posibilă, limbajul documentului a fost editat de mai multe persoane, predominant de Grace Marshall, asigurând claritate și coerență pe tot parcursul publicației. În calitate de secretar general al Coaliției Globale pentru Combaterea Criminalității Financiare, ea a ajutat la adaptarea informațiilor pentru un public larg.

Pe lângă doamna Marshall, Denisse Rudich a oferit multe ore de sprijin în evaluarea și editarea documentului, contribuind cu experiența sa vastă în domeniu dat. Cunoștințele ei atât în privința conținutului, cât și a limbajului, au fost indispensabile.

Sprijin editorial suplimentar a fost oferit de Greta Barkauskienė, Emilia Pachomow, Sungyong Kang și Vincent Danjean. Revizuirea suplimentară și sugestiile de modificări au fost efectuate de Centrul INTERPOL pentru Infracțiuni Financiare și Anticorupție (IFCACC), în special de Mona Hessein, precum și de membri ai Centrului European de Combatere a Criminalității Informatice (EC3), în special Gert Jan van Hardeveld.

Echipa OCEEA a OSCE este recunoscătoare pentru un sprijin atât de puternic.

Mulțumim sincer Unității de Informații Financiare din Letonia pentru rolul crucial în identificarea și selectarea liderilor ecosistemului pentru organizarea unei vizite de studiu axate pe activele virtuale în țările baltice. De asemenea, mulțumim Ministerului de Finanțe din Polonia pentru sprijinul continuu acordat în oferirea de spații pentru cursuri de formare. În plus, suntem profund recunoscători numeroaselor instituții și persoane dintr-o gamă largă de sectoare ale căror contribuții au fost esențiale în progresul cu succes al proiectului.

Note

OSCE Secretariat
Office of the Co-ordinator of OSCE Economic and Environmental Activities
Economic Governance Unit
Wallnerstrasse 6
1010 Vienna, Austria
E-mail: virtualassets@osce.org
www.osce.org/eea

Organization for Security and Co-operation in Europe