GHID PRIVIND INDICATORI DE SUSPICIUNE ȘI TIPOLOGII DE SPĂLARE A BANILOR ÎN DOMENIUL CRIPTO-ACTIVELOR

2023

Oficiul Național de Prevenire și Combatere a Spălării Banilor

Cuvânt înainte

Adrian CUCU

Președintele Oficiului Național de Prevenire și Combatere a Spălării Banilor

Într-o eră în care tehnologia avansează rapid și mediul financiar se transformă, este esențial să ne adaptăm și să dezvoltăm măsuri eficiente pentru a contracara amenințările asociate cu utilizarea cripto-activelor în scopuri ilegale. Spălarea banilor a devenit o preocupare majoră, iar domeniul cripto-activelor prezintă un teren fertil pentru infractori, datorită caracteristicilor sale anonime și descentralizate.

Acest ghid reprezintă rezultatul eforturilor noastre de a furniza informații relevante și soluții practice în prevenirea și combaterea spălării banilor în domeniul cripto-activelor. Prin intermediul acestui ghid, ne propunem să sporim gradul de conștientizare și să informăm instituțiile financiare, autoritățile de reglementare și pe toți cei implicați în acest domeniu cu privire la riscurile și provocările asociate fenomenului spălării banilor.

Vă încurajez să studiați cu atenție acest ghid și să-l utilizați ca un instrument esențial în lupta împotriva spălării banilor în mediul cripto-activelor. Prin colaborarea strânsă și implicarea activă, putem asigura un sistem financiar sigur și sănătos.

CUPRINS

I

Scopul ghidului

Scopul ghidului este cel de a furniza un instrument util și informativ pentru profesioniștii din domeniul cripto-activelor, precum și pentru autoritățile de reglementare și alte entități interesate. Ghidul își propune să ofere o înțelegere clară a indicatorilor de suspiciune și tipologiilor asociate spălării banilor în domeniul cripto-activelor și să ofere instrumente practice pentru identificarea și raportarea activităților suspecte.

Prin intermediul acestui ghid, cititorii vor obține cunoștințe despre legislația și reglementările relevante referitoare la combaterea spălării banilor în sectorul cripto-activelor. Vor fi prezentate definiții și termeni cheie utilizate în contextul spălării banilor în acest domeniu, asigurând astfel o bază solidă de înțelegere.

Un aspect important abordat în acest ghid este identificarea și interpretarea indicatorilor de suspiciune în tranzacțiile cu cripto-active. Prin prezentarea principiilor și metodelor utilizate în acest proces, ghidul oferă cititorilor instrumentele necesare pentru a detecta activitățile suspecte și pentru a lua măsuri corespunzătoare.

De asemenea, ghidul se concentrează și pe prezentarea alertelor (red flags) care pot indica existența unor tranzacții sau comportamente suspecte în domeniul cripto-activelor. Exemple concrete și scenarii relevante vor fi prezentate pentru a ilustra aceste indicii și pentru a ajuta cititorii să le recunoască și să le raporteze în mod adecvat.

Pe lângă analizarea indicatorilor de suspiciune și a semnalelor de alarmă, ghidul va explora diverse tipologii de spălare a banilor în domeniul cripto-activelor. Vom prezenta exemple și studii de caz relevante pentru a evidenția modurile în care cripto-activele pot fi utilizate în scopuri ilegale și pentru a masca urmele activităților ilegale. Astfel, cititorii vor obține o înțelegere mai detaliată a strategiilor și tehnicilor folosite de infractori pentru a spăla banii prin intermediul cripto-activelor.

În final, ghidul va trage concluziile principale și va evidenția importanța colaborării între instituțiile financiare, autoritățile de reglementare și organizațiile din domeniul cripto-activelor pentru a combate eficient spălarea banilor în această industrie. De asemenea, vor fi abordate perspectivele și provocările viitoare în domeniul combaterii spălării banilor în cripto-active, având în vedere evoluția rapidă a tehnologiei, precum și adaptarea continuă a infractorilor.

Scopul final al acestui ghid este de a contribui la consolidarea eforturilor de combatere a spălării banilor în domeniul cripto-activelor și de a promova un mediu financiar transparent și sigur. Prin înțelegerea mai profundă a indicatorilor de suspiciune și a tipologiilor asociate, profesioniștii din domeniul cripto și autoritățile de reglementare pot identifica mai eficient activitățile ilegale și pot implementa măsuri adecvate pentru prevenirea și combaterea spălării banilor.

Este important de subliniat faptul că acest ghid nu reprezintă o consultanță juridică sau financiară și că utilizatorii sunt încurajați să consulte specialiști în domeniu pentru interpretarea și aplicarea reglementărilor specifice. Ghidul oferă însă o bază solidă de cunoștințe și instrumente practice pentru a spori nivelul de conștientizare și a contribui la eforturile de combatere a spălării banilor în domeniul cripto-activelor.

Importanța combaterii spălării banilor în domeniul cripto-activelor

Spălarea banilor în domeniul cripto-activelor constituie o problemă semnificativă în contextul expansiunii rapide a utilizării și a popularității cripto-activelor. Această preocupare derivă din caracteristicile virtuale ale cripto-activelor și din nivelul de anonimat asociat, care pot oferi oportunități infracționale, cum ar fi finanțarea terorismului, traficul de droguri, evaziunea fiscală și alte activități ilegale din sfera financiară.

Conform unui studiu efectuat de Europol, cripto-activele reprezintă o inovație tehnică și financiară cu un mare potențial pentru economia globală. Totuși, în absența unei reglementări eficiente, acestea pot fi utilizate și în scopuri criminalle.

Pe măsură ce utilizarea cripto-activelor continuă să crească, importanța combaterii spălării banilor în acest domeniu devine fundamentală. Tehnologia cripto a captat atenția atât a investitorilor legitimi, cât și a infractorilor, datorită avantajelor pe care le oferă. Cripto-active precum Bitcoin, Ethereum, Ripple, etc permit anonimitatea, transferul rapid și global al valorii, făcându-le astfel atrăgătoare pentru activitățile de spălare a banilor. Prin urmare, este esențial să se dezvolte și să se implementeze măsuri eficiente pentru a contracara utilizarea cripto-activelor în scopuri ilegale și pentru a asigura un mediu financiar sigur și transparent.

De asemenea, este important să înțelegem că spălarea banilor în domeniul cripto-activelor are impact nu doar asupra integrității sistemului financiar, ci și asupra mediului de afaceri, stabilității economice și societății în ansamblu. Aceste practici ilegale pot submina încrederea publicului în cripto-active și pot impune riscuri financiare și juridice asupra actorilor legitimi din industrie.

O altă provocare specifică în combaterea spălării banilor în domeniul cripto-activelor constă în evoluția rapidă a tehnologiei și a metodelor utilizate de infractori. Aceștia își adaptează constant strategiile pentru a profita de caracteristicile cripto-activelor și pentru a evita detectarea. Prin urmare, eforturile de combatere a spălării banilor trebuie să fie agile, proactive și în pas cu noile tendințe și inovații tehnologice.

Pentru a contracara aceste amenințări, este crucială colaborarea între instituțiile financiare, autoritățile de reglementare, organizațiile din domeniul cripto-activelor și alte părți implicate. Prin schimbul de informații și bune practici între aceste entități, se pot dezvolta strategii eficiente de prevenire și combatere a spălării banilor în domeniul cripto-activelor. Această colaborare este vitală pentru a asigura un mediu financiar sigur și pentru a proteja integritatea sistemului financiar global.

Un aspect important de subliniat este cel referitor la necesitatea unei reglementări adecvate și actualizate în domeniul cripto-activelor. Legislația și reglementările clare și coerente pot asigura un mediu de afaceri transparent, responsabil și sigur pentru toți participanții din industrie. În acest sens, autoritățile de reglementare au un rol crucial în supravegherea și aplicarea acestor norme pentru a preveni utilizarea cripto-activelor în scopuri ilegale.

Promovarea prevenirii și combaterii spălării banilor în domeniul cripto-activelor contribuie la construirea unei baze solide de încredere în această industrie și la crearea condițiilor favorabile pentru inovație și creștere sustenabilă. În plus, implementarea unei reglementări și monitorizări eficiente este crucială pentru dezvoltarea unei industrii cripto transparente, sigure și responsabile.

Un alt scop important al luptei împotriva spălării banilor în cazul criptomonedelor este acela de a proteja utilizatorii și investitorii legitimi. Prin identificarea și eliminarea activităților ilegale și a schemelor de spălare a banilor, se poate reduce riscul de fraude și pierderi financiare pentru participanții legitimi din piață. Aceasta creează un mediu mai sigur și mai transparent pentru utilizatorii cripto-activelor și încurajează adoptarea acestora în mod responsabil și sustenabil.

Rolul Oficiului Național de Prevenire și Combatere a Spălării Banilor

Oficiul Național de Prevenire și Combatere a Spălării Banilor (O.N.P.C.S.B.) este Unitatea de Informații Financiare a României (FIU) de tip administrativ, cu rol de lider în elaborarea, coordonarea și implementarea sistemului de combatere a spălării banilor și finanțării terorismului la nivel național.

Activitatea sa a început încă din anul 1999, funcționând ca organ cu personalitate juridică, independent și autonom din punct de vedere operațional și funcțional, în prezent aflat în subordinea Ministerului Finanțelor, care în conformitate cu prevederile Legii nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finațării terorismului precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare, are ca obiect de activitate primirea, analizarea, prelucrarea și diseminarea informațiilor cu caracter financiar, precum și supravegherea și controlul, conform legii, al entităților raportoare în scopul prevenirii și combaterii spălării banilor și a finanțării terorismului.

Definiții și termeni cheie

TERMEN	DEFINIȚIE
BLOCKCHAIN	Tehnologie de înregistrare distribuită, care stochează tranzacțiile în blocuri legate între ele prin criptografie. Blockchain-ul asigură transparența și integritatea tranzacțiilor cripto.
CRIPTO-ACTIVE	Forme de valori digitale, care utilizează criptografia pentru a securiza tranzacțiile și a controla crearea de unități suplimentare (criptomonede, diverse tipuri de token-uri, NFT-uri, etc.)
CRIPTOMONEDĂ	Subcategorie distinctă de cripto-active, tip de monedă digitală, virtuală, nebancară, folosită ca mijloc de plată (ex: Bitcoin, Ethereum, Ripple, Avalanche). Criptomonedele au propriul blockchain și utilizează criptografia pentru a securiza tranzacțiile și a controla generarea de noi unități.
KYC	”Cunoaște-ți Clientul” este procesul prin care instituțiile financiare identifică și verifică identitatea clienților lor, în conformitate cu reglementările anti-spălare de bani și cunoaștere a clienților.
VASP (VIRTUAL ASSETS SERVICE PROVIDER - FURNIZOR DE ACTIVE VIRTUALE)	Furnizori de servicii legate de activele virtuale (cripomonedele) și includ platformele de schimb (exchanges), furnizorii de portofele digitale, intermediari financiari și alte entități care oferă servicii de administrare și transfer de cripto-active. Aceste entități sunt supuse unor reguli și reglementări specifice în ceea ce privește prevenirea spălării banilor și combaterea finanțării terorismului.

II Cadru legal

1. Reglementările internaționale relevante

- Standardele Grupului de Acțiune Financiară (FATF);
- Directive și regulamente ale Comisiei Europene.

2. Legislația națională (România)

- Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare;
- Ordonanţa de urgenţă nr. 53/2022 privind modificarea şi completarea Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative, cu modificările și completările ulterioare;;
- Hotărârea de Guvern nr. 603/2011 pentru aprobarea Normelor privind supravegherea de către Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor a modului de punere în aplicare a sancţiunilor internaţionale, modificată prin Hotărârea nr. 299/2021;
- Ordinul presedintelui O.N.P.C.S.B. nr. 37/2021 privind aprobarea Normelor de aplicare a prevederilor Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative, cu modificările și completările ulterioare, pentru entităţile raportoare supravegheate şi controlate de catre O.N.P.C.S.B.

3. Obligațiile entităților raportoare în domeniul cripto-activelor în privința combaterii spălării banilor

1. Reglementările internaționale relevante

Grupul de Acțiune Financiară (GAFI) - FATF, este o organizație internațională care colaborează cu statele membre pentru a monitoriza și promova implementarea recomandărilor sale în domeniul cripto-activelor. Aceste recomandări reprezintă un set de standarde și obligații care au ca scop combaterea spălării banilor și finanțării terorismului, în toate domeniile, inclusiv în acest sector emergent.

Recomandările FATF în ceea ce privește cripto-activele cuprind diverse aspecte importante, printre acestea numărându-se obligația entităților de a identifica și verifica identitatea clienților lor, de a supraveghea activitățile desfășurate și de a raporta orice tranzacții suspecte autorităților competente. Prin implementarea acestor recomandări, țările membre sunt încurajate să creeze un mediu reglementat și transparent în care cripto-activele să poată funcționa în conformitate cu legile și regulamentele internaționale împotriva spălării banilor.

FATF are un rol important în promovarea cooperării internaționale și a schimbului de informații între statele membre. Prin intermediul evaluărilor și rapoartelor periodice, FATF monitorizează progresele realizate de către țările membre în implementarea recomandărilor și identifică eventualele lacune sau zone de îmbunătățire.

De asemenea, **Comisia Europeană** joacă un rol semnificativ în reglementarea domeniului cripto-activelor în cadrul Uniunii Europene. Comisia lucrează la dezvoltarea unui cadru legal și reglementar coerent și armonizat în întreaga regiune. Aceasta își propune să consolideze securitatea și integritatea pieței, să protejeze investitorii și să prevină utilizarea cripto-activelor în scopuri ilegale, inclusiv spălarea banilor și finanțarea terorismului.

Unul dintre obiectivele Comisiei Europeane este cel de a crea un mediu reglementat și transparent în care operatorii din domeniul cripto-activelor să acționeze conform standardelor ridicate de integritate și siguranță. Acest lucru dorește a spori încrederea investitorilor și stimulează adopția largă a cripto-activelor în economia europeană.

Astfel, prin implicarea organizațiilor și instituțiilor internaționale precum FATF și Comisia Europeană, reglementările internaționale relevante în domeniul cripto-activelor sunt promovate și implementate. Aceste reglementări și acțiuni de supraveghere contribuie la crearea unui mediu reglementat, transparent și sigur pentru cripto-activități, asigurând protecția investitorilor și prevenirea utilizării cripto-activelor în scopuri ilegale.

2. Legislația națională (România)

Conform art. 5 alin. (1), lit. g[1] și g[2]din **Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului**, precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare, furnizorii de servicii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale sunt considerați entități raportoare, supravegheate de O.N.P.C.S.B., ceea ce înseamnă că acestora le revine obligația legală de a raporta tranzacțiile suspecte sau neobișnuite și de a coopera cu Oficiul în îndeplinirea atribuțiilor sale.

Prin **Ordonanța de Urgență nr. 53/2022**, se stabilește obligația entităților raportoare prevazute la art. 5 alin. (1), lit. g)-k) din Legea nr. 129/2019, cu modificările și completările ulterioare, inclusiv furnizorii de servicii de schimb între monede virtuale şi monede fiduciare şi furnizorii de portofele digitale, de a notifica Oficiul, exclusiv în format electronic, cu privire la începerea, suspendarea sau încetarea activității, în termen de 15 zile de la data începerii, suspendării sau încetării activității. Această măsură are ca scop, din perspectiva Oficiului Național de Prevenire și Combatere a Spălării Banilor, cunoașterea dimensiunii sectorului și monitorizarea entităților raportoare, iar din perspectiva entității raportoare, se dorește a fi modalitatea prin care persoanele implicate devin conștiente de importanța obligațiilor ce le revin și de riscurile la care sunt expuse.

Hotărârea de Guvern nr. 603/2011, modificată prin **Hotărârea nr. 299/2021**, reprezintă actul normativ prin care sunt aprobate Normele privind supravegherea de către Oficiul Național de Prevenire și Combatere a Spălării Banilor a modului de punere în aplicare a sancțiunilor internaționale. Aceasta reglementează procedurile și responsabilitățile entităților implicate în monitorizarea și aplicarea sancțiunilor internaționale în contextul combaterii spălării banilor și finanțării terorismului, asigurând astfel conformitatea României cu standardele internaționale în domeniu.

Ordinul președintelui O.N.P.C.S.B. nr. 37/2021 privind aprobarea Normelor de aplicare a prevederilor Legii nr. 129/2019 stabilește cadrul și regulile specifice pe care entitățile raportoare trebuie să le urmeze în vederea conformării la legislația națională în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului (identificarea și verificarea clienților, monitorizarea tranzacțiilor, raportarea operațiunilor cu numerar, raportarea tranzacțiilor suspecte etc).

Actele normative menționate, precum și alte documente relevante în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, pot fi accesate și consultate pe site-ul oficial al Oficiului Național de Prevenire și Combatere a Spălării Banilor (ONPCSB), la adresa www.onpcsb.ro.

3. Obligațiile entităților raportoare în domeniul cripto-activelor în privința combaterii spălării banilor

Conform Legii nr. 129/2019, toate entitățile raportoare, inclusiv furnizorii de schimb între monede virtuale și monede fiduciare, precum și furnizorii de portofele digitale, au obligații specifice în privința combaterii spălării banilor în domeniul cripto-activelor, precum:

- **Identificarea și verificarea clienților**: entitățile raportoare sunt responsabile de identificarea și verificarea identității clienților lor înainte de a iniția tranzacții cu cripto-active, inclusiv colectarea și înregistrarea informațiilor esențiale, cum ar fi numele, adresele și informațiile de identificare;

- **Monitorizarea tranzacțiilor suspecte:** entitățile raportoare trebuie să monitorizeze tranzacțiile efectuate cu cripto-active și să identifice tranzacțiile care prezintă indicii de spălare a banilor sau finanțare a terorismului. În astfel de cazuri, acestea au obligația de a raporta tranzacțiile suspecte către Oficiul Național de Prevenire și Combatere a Spălării Banilor;

- **Păstrarea documentelor și a înregistrărilor:** entitățile raportoare trebuie să păstreze documentele și înregistrările referitoare la tranzacțiile cu cripto-active și informațiile despre clienți, pentru a permite verificarea ulterioară și a facilita investigațiile în caz de suspiciuni de spălare a banilor sau finanțare a terorismului;

- **Furnizarea de informații:** entitățile raportoare sunt obligate să ofere informații solicitate de Oficiul Național de Prevenire și Combatere a Spălării Banilor cu privire la activitățile lor și la tranzacțiile cu cripto-active;

- **Instruirea personalului:** entitățile raportoare trebuie să asigure instruirea și conștientizarea personalului lor cu privire la riscurile de spălare a banilor și finanțare a terorismului în domeniul cripto-activelor și să pună în aplicare măsuri adecvate pentru prevenirea acestor activități ilegale.

Aceste obligații au fost impuse pentru a asigura conformitatea cu standardele internaționale în materie de prevenire și combatere a spălării banilor și finanțării terorismului și pentru a promova un mediu reglementat și transparent în industria cripto-activelor.

Toate obligațiile entităților raportoare în domeniul cripto-activelor în privința combaterii spălării banilor pot fi consultate în Legea nr. 129/2019.

III

Indicatori de suspiciune

În contextul dinamic al domeniului cripto-activelor, riscul spălării banilor și finanțării terorismului a devenit o preocupare majoră pentru entitățile raportoare și pentru autoritățile de reglementare. Cripto-activele oferă oportunități unice pentru transferul rapid și anonim de valoare, ceea ce poate facilita activități ilegale și nereglementate. Pentru a contracara aceste riscuri, este esențial să se identifice și să se combată activitățile suspecte prin utilizarea indicatorilor de suspiciune.

Capitolul III, bazat pe informările primite de Oficiul Național de Prevenire și Combatere a Spălării Banilor, se concentrează pe principiile și metodele de identificare a activităților suspecte în tranzacțiile cu cripto-active. Din analiza acestor informări, au fost identificați indicatori de suspiciune cu o frecvență mai ridicată.

Entitățile raportoare trebuie să fie proactive în identificarea tranzacțiilor și comportamentelor care ridică suspiciuni. Acest lucru poate fi realizat prin analiza detaliată a tranzacțiilor, monitorizarea activității clienților, identificarea schemelor de tranzacționare neobișnuite și a altor modele care pot semnala activități ilegale sau nefirești. În plus, capitolul abordează comportamentele și modelele de tranzacții care ar putea ridica suspiciuni.

De asemenea, tehnologiile avansate, precum analiza blockchain și analiza de date, pot fi folosite pentru a urmări tranzacțiile și a identifica modele, conexiuni și comportamente suspecte.

1. Principii și metode de identificare a activităților suspecte în tranzacțiile cu cripto-active

Pentru a identifica activitățile suspecte în tranzacțiile cu cripto-active, entitățile raportoare și autoritățile de reglementare se bazează pe anumite principii și metode. Acestea includ:

- **Monitorizarea tranzacțiilor:** entitățile raportoare au responsabilitatea de a monitoriza în mod constant tranzacțiile cu cripto-active, cu scopul de a identifica comportamente sau modele neobișnuite, ceea ce implică analizarea volumului tranzacțiilor, frecvenței, valorilor implicate și participanților implicați în aceste tranzacții;

- **Cunoașterea clientelei:** o componentă esențială în identificarea activităților suspecte este cunoașterea clienților. Entitățile raportoare trebuie să obțină și să verifice informațiile relevante despre clienți, inclusiv identitatea lor, scopul tranzacțiilor și sursa fondurilor implicate;

- **Analiza tranzacțiilor în raport cu profilul clientului:** prin compararea tranzacțiilor unui client cu profilul său obișnuit de tranzacționare, se pot identifica discrepanțe sau abateri care pot ridica suspiciuni. Aceasta implică evaluarea volumului, frecvenței, direcției și altor caracteristici ale tranzacțiilor în raport cu comportamentul anterior al clientului.

- **Colaborarea și schimbul de informații:** entitățile raportoare și autoritățile de reglementare trebuie să colaboreze și să schimbe informații pentru a identifica și combate activitățile suspecte, prin raportarea tranzacțiilor suspecte și partajarea de date relevante între ele.

2. Comportamente și modele de tranzacții care ar putea ridica suspiciuni

În domeniul cripto-activelor, există anumite comportamente și modele de tranzacții care pot ridica suspiciuni și necesită o atenție specială. Acestea pot include:

- **Tranzacții de mare valoare:** tranzacțiile cu cripto-active de valoare mare, care depășesc anumite limite financiare semnificative, pot fi considerate a fi un puternic indicator de suspiciune, deoarece acestea pot fi adesea asociate cu activități ilegale sau cu intenția de a ascunde fonduri ilicite;

- **Transferuri frecvente și rapide:** tranzacțiile care implică transferuri frecvente și rapide de cripto-active pot ridica suspiciuni, deoarece pot indica o încercare de a ascunde fluxul de fonduri sau de a evita detecția;

- **Utilizarea mixerelor de cripto-active:** mixerele de cripto-active sunt servicii utilizate pentru a amesteca și anonimiza tranzacțiile, făcându-le mai greu de urmărit. Utilizarea frecventă a mixerelor de cripto-active poate fi un indicator de suspiciune;

- **Transferuri către adrese necunoscute sau suspecte:** transferurile către adrese necunoscute sau suspecte în domeniul cripto-activelor pot ridica suspiciuni în privința legalității tranzacțiilor. Aceste adrese pot fi asociate cu activități ilegale, precum utilizarea dark web-ului, ransomware-ul sau traficul de droguri, ceea ce indică un posibil caracter ilicit al tranzacțiilor. Prin urmare, entitățile raportoare trebuie să acorde o atenție specială acestor transferuri și să evalueze riscurile asociate în cadrul procesului lor de monitorizare și identificare a activităților suspecte;

- **Tranzacții către țări cu legislație permisivă în privința spălării banilor:** Astfel de tranzacții pot fi folosite în mod intenționat pentru a ascunde fonduri ilicite sau pentru a evita atenția autorităților de supraveghere și reglementare. Prin urmare, acestea pot ridica preocupări semnificative cu privire la legalitatea și transparența tranzacțiilor respective.

3. Utilizarea tehnologiilor de urmărire și analiză a tranzacțiilor

Pentru a sprijini identificarea și combaterea activităților suspecte în tranzacțiile cu cripto-active, entitățile raportoare utilizează tehnologii de urmărire și analiză a tranzacțiilor. Aceste tehnologii pot include:

- **Soft-uri de analiză a tranzacțiilor pe blockchain:** prin utilizarea tehnologiei blockchain, care stă la baza cripto-activelor, se poate realiza o înregistrare transparentă și descentralizată a tranzacțiilor. Analiza blockchain-ului devine astfel un instrument valoros în identificarea tranzacțiilor suspecte și în urmărirea fluxului de fonduri, facilitând combaterea spălării banilor și a activităților ilegale;

- **Algoritmi de analiză și inteligență artificială:** utilizarea algoritmilor de analiză și inteligență artificială poate spori capacitatea de identificare a activităților suspecte prin analizarea modelelor de tranzacții, a comportamentului clienților și a altor factori relevanți;

- **Cooperarea cu furnizorii de servicii de urmărire a cripto-activelor:** entitățile raportoare pot colabora cu furnizorii specializați în urmărirea și analiza tranzacțiilor cu cripto-active. Acești furnizori pot oferi instrumente și servicii avansate pentru identificarea și monitorizarea activităților suspecte, inclusiv analiza tranzacțiilor, investigarea adresei IP, urmărirea surselor de fonduri și detecția comportamentului neobișnuit;

- **Utilizarea bazelor de date și a informațiilor de tip Know Your Customer (KYC):** entitățile raportoare pot utiliza baze de date și informații KYC pentru a verifica identitatea clienților și a evalua riscurile asociate cu aceștia. Aceste informații pot ajuta la identificarea tranzacțiilor suspecte și a activităților ilegale.

Colaborarea între entitățile raportoare și autoritățile de reglementare este esențială în acest proces pentru a asigura o supraveghere eficientă și pentru a menține integritatea și transparența pieței cripto-activelor.

IV

Tipologii de spălare de bani în domeniul cripto-activelor

În era digitală, spălarea de bani a devenit o amenințare semnificativă, iar domeniul cripto-activelor a deschis noi oportunități pentru infractori să-și ascundă și să-și curețe fondurile ilicite. Capitolul IV se axează pe explorarea tipologiilor specifice de spălare de bani în acest domeniu dinamic și în continuă evoluție.

În acest capitol vor fi analizate metodele și strategiile utilizate de către infractori pentru a transforma fondurile obținute din activități ilegale în cripto-active aparent legale. Aceste tipologii sunt rezultatul adaptării și inovării în contextul tehnologiei blockchain și a caracteristicilor specifice cripto-activelor, care facilitează anonimitatea și dificultatea de urmărire a tranzacțiilor.

Obiectivul este de a dezvălui și de a înțelege aceste tipologii, oferind exemple concrete și informații bazate pe cercetări și studii relevante. Acest aspect va permite identificarea comportamentelor și modelelor specifice asociate cu spălarea de bani în domeniul cripto-activelor și dezvoltarea de strategii eficiente pentru combaterea acestui fenomen.

Prin analiza atentă a acestor tipologii, se urmărește senzibilizarea atât a entităților raportoare, cât și a autorităților de reglementare cu privire la riscurile și provocările asociate cu spălarea banilor în domeniul cripto-activelor.

01 Utilizarea platformelor neconforme sau fără licență

Spălarea de bani directă prin tranzacții cu cripto-active reprezintă procesul prin care fondurile ilicite sunt introduse în mediul cripto, transferate prin multiple tranzacții pentru a ascunde originea lor și apoi convertite în cripto-active curate.

02 Utilizarea cărăușilor de bani în spălarea de bani

Utilizarea cărăușilor de bani în spălarea banilor în domeniul cripto-activelor se referă la implicarea persoanelor intermediare în procesul de transfer și conversie a fondurilor ilicite, cu scopul de a ascunde traseul și beneficiarii finali ai acestor fonduri.

03 Utilizarea mixerelor și a platformelor DeFi pentru ascunderea urmelor

Reprezintă o tehnică folosită în spălarea de bani în domeniul cripto-activelor, în care tranzacțiile sunt amestecate și transferate prin intermediul platformelor descentralizate pentru a crește dificultatea identificării și urmăririi originii și destinației fondurilor.

04 Utilizarea ATM-urilor de cripto în scopul spălării banilor

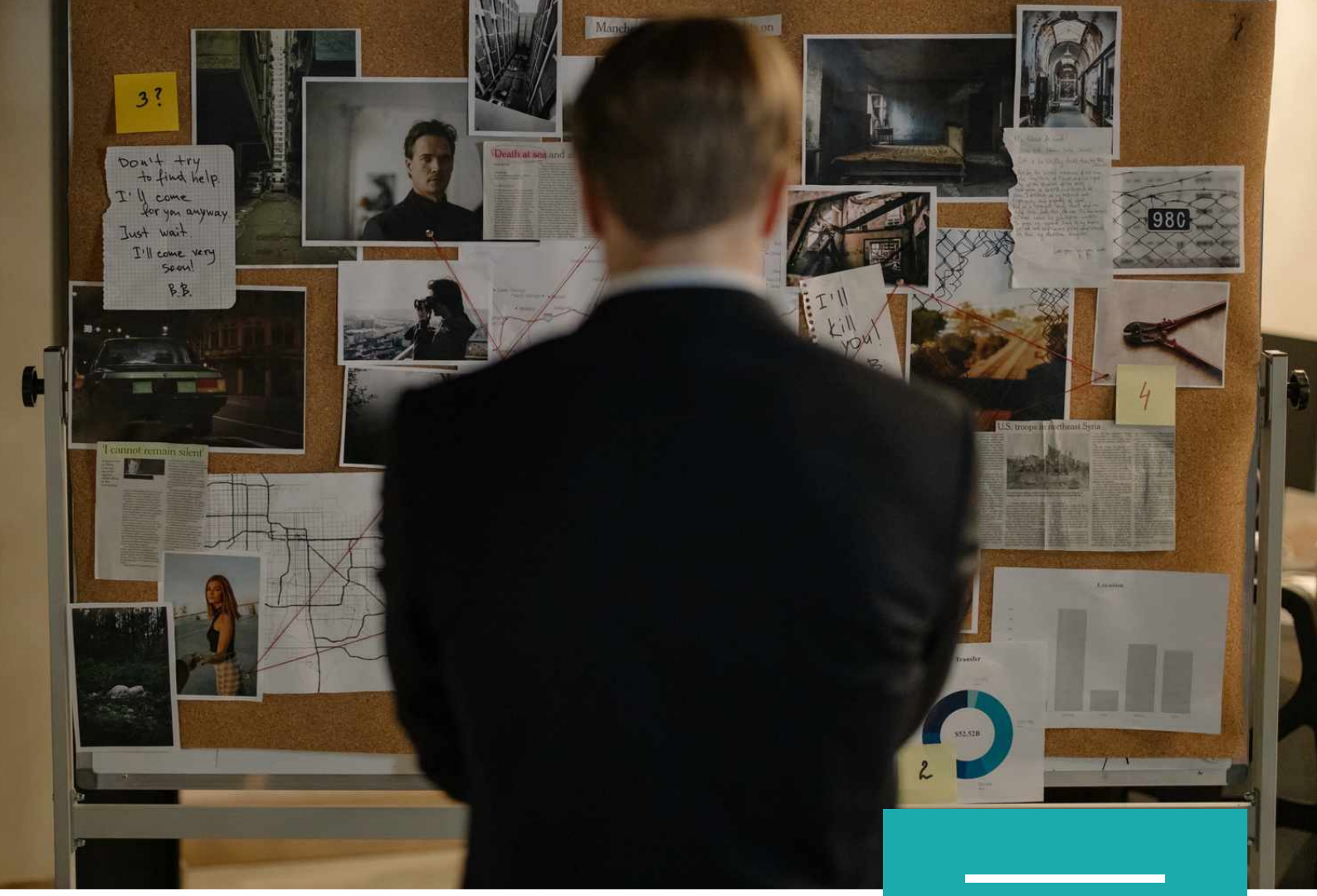
Reprezintă o metodă prin care fondurile ilicite sunt convertite în cripto-active prin intermediul automatelor cripto, oferindu-le infractorilor posibilitatea de a obține fonduri "curate" într-un mod aparent legal și fără a dezvălui identitatea lor.

05 Utilizarea NFT-urilor în scopul spălării banilor

Utilizarea NFT-urilor în scopul spălării banilor implică transferul fondurilor ilicite prin intermediul acestor active digitale unice, care permit infractorilor să ascundă originea ilicită și să spele fondurile, profitând de caracteristicile speciale și dificultatea de urmărire asociate cu acestea.

06 Utilizarea ICO-urilor în scopul spălării banilor

Utilizarea ICO-urilor în scopul spălării banilor constă în lansarea de campanii de finanțare colectivă prin intermediul cripto-activelor, prin care infractorii își ascund originile fondurilor ilicite și obțin aparența legalității prin intermediul investițiilor și tranzacțiilor cripto.



1. Utilizarea platformelor neconforme sau fără licență

Una dintre metodele comune de spălare a banilor prin tranzacții cu cripto-active implică utilizarea platformelor de schimb neconforme șau fără licență. Infractorii exploatează vulnerabilitățile acestor platforme, care adesea nu implementează măsuri de cunoaștere a clientelei (KYC) și nu se conformează reglementărilor din jurisdicțiile specifice.

Platformele de schimb neconforme sau fără licență oferă un mediu propice pentru spălarea banilor, deoarece nu solicită informații detaliate despre identitatea clienților sau despre originea fondurilor. Acestea tind să evite aplicarea rigorilor reglementărilor anti-spălare de bani și a standardelor KYC, facilitând astfel utilizarea de conturi anonime sau cu informații de identificare minime, permițând infractorilor să efectueze tranzacții fără a fi supuși unei verificări adecvate a identității lor și fără a fi înregistrate detaliile relevante în scopul de a identifica activitățile ilicite. De asemenea, aceste platforme nu aplică restricții privind volumul și valorile tranzacțiilor, oferind astfel posibilitatea infractorilor de a efectua tranzacții mari și frecvente fără a atrage atenția autorităților.

Descrierea tipologiei

1. Un individ obține cripto-active prin intermediul unui atac ransomware, care constă în preluarea controlului asupra sistemelor informatice ale victimelor și în solicitarea unei răscumpărări în cripto-active. După obținerea cripto-activelor, infractorul urmărește să le legalizeze prin scheme complexe de spălare a banilor, cum ar fi schimburile succesive pe platforme neconforme, pentru a ascunde urma tranzacțiilor și pentru a îngreuna urmărirea activităților ilicite;

2. Primul pas în procesul de spălare a banilor constă în **identificarea unei platforme de schimb neconforme sau fără licență și deschiderea unui cont anonim pe aceasta**. Prin deschiderea unui cont anonim, persoana evită furnizarea de informații detaliate despre identitatea sa, ceea ce îi permite să efectueze tranzacții fără a fi supus unei verificări adecvate a identității și fără a lăsa urme digitale care ar putea duce la identificarea sa. Alegerea unei astfel de platforme neconforme sau fără licență este esențială, deoarece aceasta oferă un grad mai mare de anonimat și reduce riscul de a fi detectat de către autorități sau instituțiile de aplicare a legii;

3. După ce cripto-activele obținute ilegal sunt transferate pe această platformă, **acestea vor fi convertite în alte active digitale sau în monede fiduciare**;

4. **Cripto-activele "murdare", transformate în alte active digitale, vor fi ulterior schimbate în monedă fiduciară prin intermediul unor tranzacții succesive**, realizate atât pe platforme neconforme sau fără licență, cât și pe platforme conforme;

5. **Fondurile rezultate din aceste schimburi de cripto-active vor fi apoi transferate într-un cont bancar sau vor fi retrase în numerar de la un automat de cripto.** Prin această etapă, infractorul încearcă să integreze fondurile obținute ilegal în sistemul financiar tradițional sau să le convertească în bani lichizi, facilitând astfel utilizarea lor în activități legale sau pentru a evita detectarea tranzacțiilor ilicite. Această acțiune adițională contribuie la crearea unei aparențe de legalitate asupra fondurilor și complică urmărirea fluxurilor de bani, adăugând un nivel suplimentar de complexitate în procesul de investigare a activităților infracționale.

Indicatori specifici tipologiei

1. Lipsa licenței și neconformitatea platformei de schimb: platforma utilizată în procesul de spălare a banilor nu este licențiată în mod oficial și nu respectă politicile și procedurile adecvate de combatere a spălării banilor. Poate fi vorba de o platformă nou înființată sau nou înregistrată;

2. Cont anonim și lipsa măsurilor de cunoaștere a clientelei: individul deschide un cont anonim pe platformă fără a furniza informații detaliate sau a fi verificat în mod adecvat. Platforma nu aplică măsuri de cunoaștere a clientelei, asigurând anonimatul persoanei;

3. Lipsa restricțiilor privind volumul și valorile tranzacțiilor: platforma de schimb neconformă sau fără licență nu impune limite sau restricții asupra volumului sau valorii tranzacțiilor efectuate. Aceasta permite individului să efectueze tranzacții mari și frecvente fără a atrage atenția autorităților;

4. Participarea frecventă a clienților la tranzacțiile derulate pe platforme neconforme: utilizatorii acestor platforme de schimb, care nu respectă reglementările și standardele KYC, sunt implicați în mod frecvent în tranzacții cu cripto-active desfășurate pe aceste platforme;

5. Mesaje sugestive și informații privind anonimatul și utilizarea numerarului: platforma de schimb afișează pe site-ul său web mesaje sugestive care promovează anonimatul utilizatorilor și menționează acceptarea numerarului în tranzacțiile cu cripto-active;

6. Servicii de chat între utilizatori: platforma de schimb neconformă oferă servicii de chat între utilizatori, creând un mediu propice pentru comunicarea și coordonarea tranzacțiilor ilegale, precum și discuții legate de activități suspecte.

7. Implicarea platformei de schimb în tranzacții cu cripto-active de proveniență ilicită: există informații care indică implicarea platformei de schimb în tranzacții cu cripto-active provenite din surse ilicite. Acest lucru poate fi relevat de investigații anterioare sau de surse de informații disponibile public.

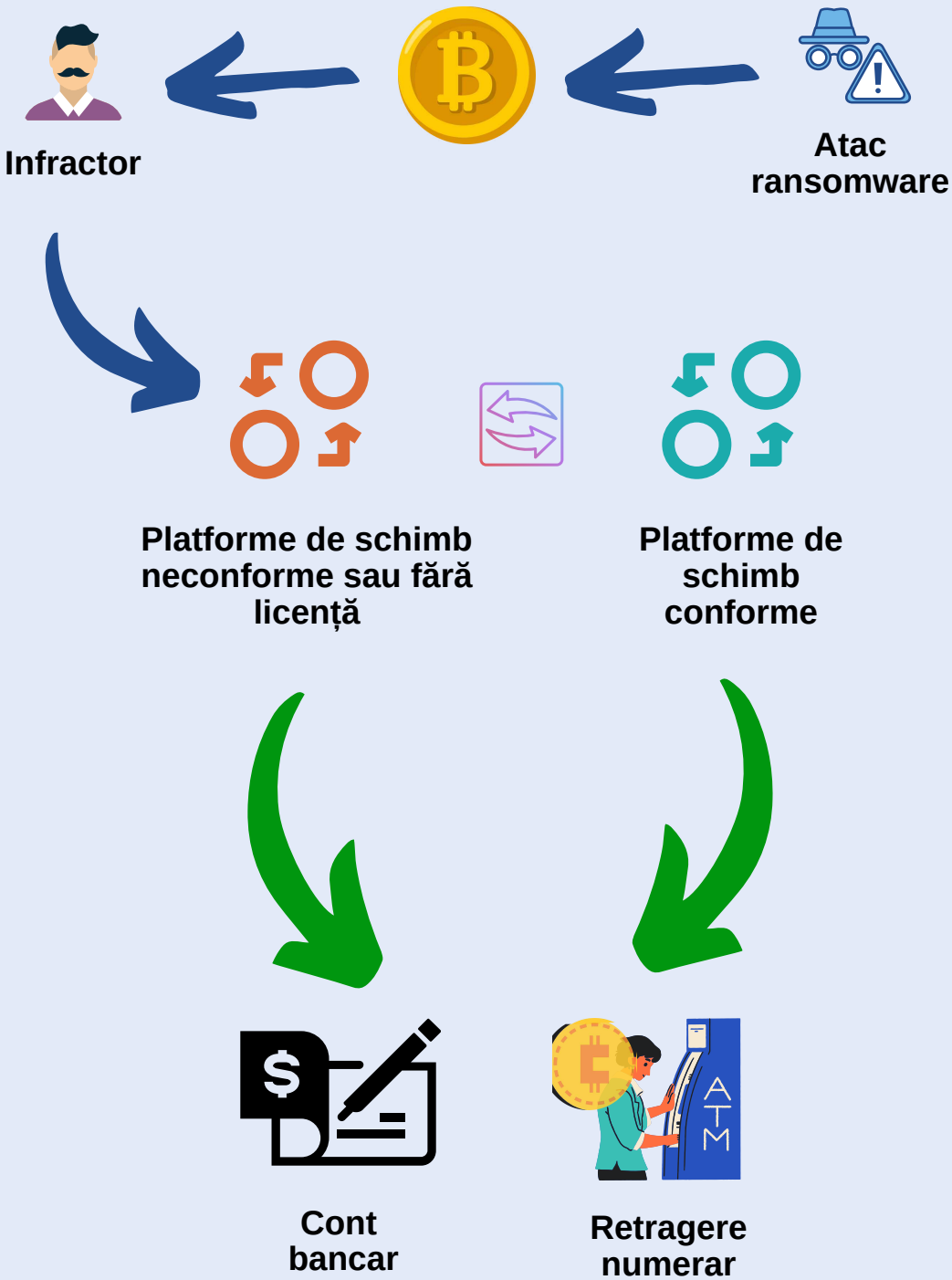
Exemple concrete:

1. Un individ care este implicat în activități ilegale, cum ar fi traficul de droguri sau infracțiunile cibernetice, utilizează o platformă de schimb neconformă pentru a spăla banii obținuți ilegal. Acesta deschide un cont pe platformă fără a furniza informații personale detaliate și efectuează tranzacții de cripto-active fără a fi supus unor verificări riguroase ale identității sale. Prin intermediul platformei neconforme, individul poate transfera și converti cripto-activele obținute ilegal, ascunzând astfel originea și urmele acestor fonduri;

2. Un individ care se ocupă cu fraudă online sau phishing utilizează o platformă neconformă pentru a transfera fondurile obținute în cripto-active. Acest individ poate utiliza o astfel de platformă pentru a efectua schimburi de cripto-active între diferite adrese anonime. Prin această metodă, individul face mai dificilă urmărirea tranzacțiilor și identificarea activităților sale ilegale. Utilizând o platformă neconformă, individul poate evita verificările stricte ale identității și furnizarea de informații personale, ceea ce îi conferă un nivel mai mare de anonimat și confidențialitate în desfășurarea activităților ilegale. Acest lucru îi permite să convertească rapid și eficient fondurile obținute în mod fraudulos în cripto-active, ceea ce face dificilă recuperarea fondurilor de către autorități.

Surse:

- *Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html;*
- *Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021*


Infractor
Atac ransomware
Platforme de schimb neconforme sau fără licență
Platforme de schimb conforme
Cont bancar
Retragere numerar
ATM

2. Utilizarea cărăușilor de bani în spălarea de bani

Spălarea de bani în domeniul cripto-activelor implică adesea utilizarea unor tactici sofisticate pentru a ascunde originile ilicite ale fondurilor și a evita detectarea de către autorități. Una dintre aceste tipologii este reprezentată de utilizarea cărăușilor de bani, cunoscuți și sub denumirea de ”money mules”.

Acești indivizi devin intermediari în transferul de fonduri ilicite, facilitând astfel spălarea și dispersia acestora prin intermediul cripto-activelor. Cărăușii de bani acceptă să primească fonduri provenite din activități ilegale în conturile lor personale sau în portofelele lor electronice, urmând apoi instrucțiunile infractorilor cu privire la transferurile și conversiile necesare pentru a ascunde urmele tranzacțiilor și a dispersa fondurile într-un mod aparent legal.

Prin implicarea cărăușilor de bani în acest proces complex, infractorii își pot spăla banii și pot beneficia de caracteristicile anonime și descentralizate ale cripto-activelor, oferindu-le o protecție suplimentară împotriva identificării și urmăririi de către autorități.

Descrierea tipologiei

1. Recrutarea cărăușilor de bani: infractorii identifică potențiali cărăuși de bani prin intermediul diferitelor canale, cum ar fi site-uri de recrutare online, platforme de socializare sau chiar prin intermediul cunoștințelor personale. Aceștia sunt atrași prin promisiuni de câștiguri rapide și ușoare sau prin oferte de "muncă" în cadrul unor companii fictive;

2. Instruirea și implicarea cărăușilor de bani se referă la faptul că aceștia sunt instruiți și li se furnizează informații personale și bancare pentru a facilita transferurile de fonduri prin conturile lor, inclusiv crearea de conturi de cripto-activeși desfășurarea tranzacțiilor în numele infractorilor;

3. Transferurile de fonduri: cărăușii de bani transferă fondurile ilicite către adresele de cripto-active specificate de infractori, folosind platforme de schimb sau portofele digitale;

4. Divizarea și disiparea fondurilor: odată ce fondurile sunt transferate către adresele de cripto-active, infractorii încearcă să disipeze și să divizeze aceste fonduri pentru a crește dificultatea urmăririi și identificării lor. Acest lucru poate implica realizarea unor tranzacții multiple și complexe între diferite adrese de cripto-active, amestecarea fondurilor prin intermediul mixerelor și utilizarea altor tactici de dispersare a fondurilor;

5. Conversia în monede fiduciare: în final, fondurile convertite în cripto-active pot fi transferate înapoi în moneda fiduciară pentru a încerca să se spargă legătura cu activitățile ilegale inițiale. Pentru a realiza aceste transferuri, infractorii pot utiliza platforme de schimb cripto-fiat sau pot recurge la tranzacții peer-to-peer, implicând persoane sau entități dispuse să efectueze schimbul monetar. Acest proces complex contribuie la dificultatea de a urmări originea și destinația finală a fondurilor;

6. Complicitatea cărăușilor de bani: este important de menționat că, în multe cazuri, cărăușii de bani pot fi conștienți sau chiar complici în activitățile ilegale în care sunt implicați, fiind motivați de profit sau manipulați prin șantaj sau amenințări.

Indicatori specifici tipologiei

1. Relații cu persoane cunoscute ca fiind implicate în activități criminale: cauza principală a implicării curierilor de bani în spălarea banilor este relația lor cu infractorii care au obținut fondurile ilegal. Acești curieri de bani au adesea conexiuni și cunoștințe în lumea infracțională, ceea ce facilitează procesul de spălare a banilor prin intermediul lor;

2. Servicii de intermediere financiară neautorizate: Curierii de bani operează adesea ca intermediari financiari neautorizați, oferind servicii de transfer de fonduri și conversie valutară în numele infractorilor. Aceștia pot acționa ca persoane fizice sau pot avea societăți fantomă prin intermediul cărora își desfășoară activitățile ilegale;

3. Tranzacții financiare neobișnuite și atipice: curierii de bani desfășoară tranzacții financiare neobișnuite și atipice care nu se încadrează în tiparele normale de afaceri. Aceste tranzacții pot include schimburi frecvente de valută, transferuri rapide și repetate de fonduri între conturi și utilizarea unor modalități complexe de a ascunde urmele transferurilor financiare;

4. Utilizarea conturilor bancare multiple: curierii de bani utilizează de obicei conturi bancare multiple pentru a dispersa și ascunde fondurile. Aceștia pot avea conturi în diferite jurisdicții și pot efectua transferuri între aceste conturi pentru a îngreuna urmărirea fluxului de bani și pentru a ascunde urmele activităților ilicite;

5. Tranzacții cu numerar: curierii de bani sunt implicați adesea în tranzacții cu numerar, deoarece oferă un nivel mai mare de anonimat și facilitează spălarea banilor prin schimburi rapide de fonduri în numerar între diferite persoane și locații;

6. Utilizarea unor scheme de structurare a tranzacțiilor: pentru a evita declanșarea rapoartelor de tranzacții financiare suspecte (RTS-uri), curierii de bani pot utiliza scheme de structurare a tranzacțiilor prin care împart sume mari de bani în tranzacții mai mici pentru a evita atragerea atenției autorităților financiare.

Exemple concrete:

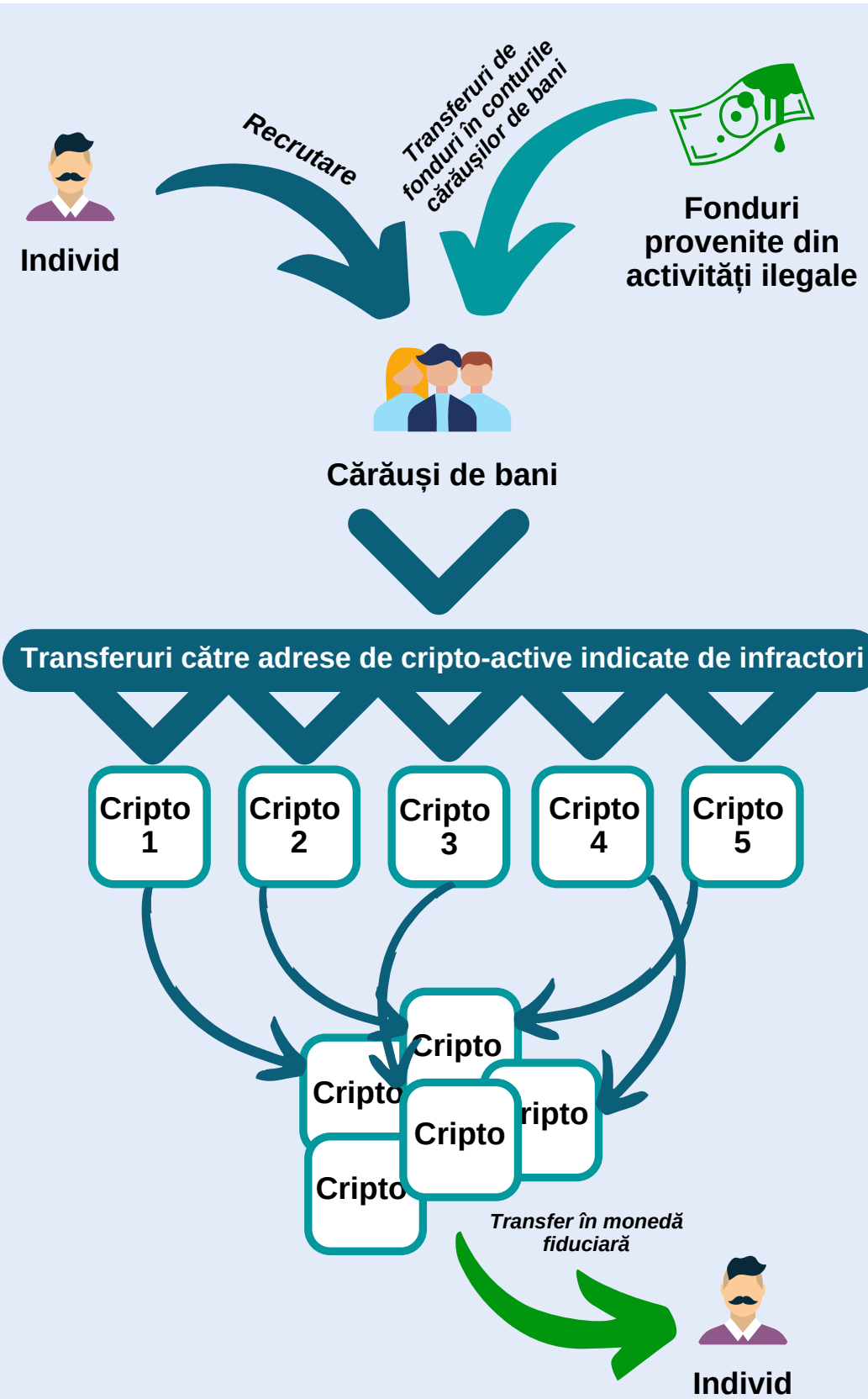
1. Un individ este recrutat pentru a transfera fonduri ilicite prin intermediul cripto-activelor către o persoană din altă țară. El primește instrucțiuni precise cu privire la conturile de cripto-active în care trebuie să efectueze transferurile și primește o parte din fonduri ca recompensă pentru serviciile sale;

2. Un grup infracțional utilizează o rețea extinsă de cărăuși de bani pentru a transfera fonduri provenite din activități de phishing și fraudă online în cripto-active. Aceștia folosesc adrese de cripto-active diverse și servicii de mixare pentru a ascunde originea fondurilor și a face dificilă urmărirea lor;

3. O companie fantomă recrutează persoane care să joace rolul de cărăuși de bani pentru a transfera fonduri ilicite prin intermediul cripto-activelor. Aceste persoane sunt implicate în crearea de conturi de cripto-active pe diferite platforme și efectuarea de tranzacții în numele companiei, fără a fi conștiente de caracterul ilegal al activităților în care sunt implicate.

Surse:

- *Elliptic Typologies Report 2022 Edition, Preventing Financial Crime in Cryptoassets;*
- *Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html;*
- *Europol - "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (2019).*


Individ
Recrutare
Transferuri de fonduri în conturile cărăușilor de bani
Fonduri provenite din activități ilegale
Cărăuși de bani
Transferuri către adrese de cripto-active indicate de infractori
Cripto 1
Cripto 2
Cripto 3
Cripto 4
Cripto 5
Cripto
Cripto
Cripto
ripto
Cripto
Transfer în monedă fiduciară
Individ

3. Utilizarea mixerelor și a platformelor DeFi pentru ascunderea urmelor

Unul dintre instrumentele folosite de infractori pentru a ascunde urmele și a spăla fondurile ilicite este utilizarea mixerelelor și a platformelor descentralizate. Mixerele, cunoscute și sub denumirea de crypto tumblers, sunt platforme specializate care permit amestecarea cripto-activelor prin combinarea și amestecarea multiplelor tranzacții, ceea ce face dificilă urmărirea originii fondurilor. Aceste mixere oferă o formă de anonimat, deoarece nu este posibilă identificarea exactă a surselor și destinațiilor tranzacțiilor.

Pe de altă parte, platformele descentralizate (DeFi) sunt platforme de tranzacționare peer-to-peer, care facilitează schimbul direct între utilizatori, eliminând intermediarii centralizați. Aceste platforme permit utilizatorilor să efectueze tranzacții fără a fi nevoie să-și dezvăluie identitatea sau să furnizeze informații personale detaliate. În plus, platformele descentralizate nu stochează fondurile utilizatorilor, ceea ce adaugă un nivel suplimentar de confidențialitate și securitate.

Descrierea tipologiei

Utilizarea mixerelelor și a platformelor descentralizate reprezintă o tipologie comună în procesul de spălare a banilor prin intermediul cripto-activelor. Această tipologie implică următorii pași:

1. Utilizarea mixerelelor: infractorul își transferă cripto-activele într-un mixer. Acesta preia cripto-activele de la utilizatori și le redistribuie într-un mod care maschează legătura dintre adresele de origine și cele de destinație. Acest proces implică de obicei mai multe tranzacții interne și schimburi între adrese diferite, ceea ce complică și mai mult urmărirea fondurilor;

2. Tranzacții anonime și lipsa verificării identității: mixerele și platformele descentralizate oferă utilizatorilor posibilitatea de a efectua tranzacții fără a fi obligați să dezvăluie informații personale detaliate sau să treacă prin verificări riguroase ale identității lor. Această caracteristică oferă utilizatorilor un nivel crescut de anonimat și confidențialitate în tranzacțiile financiare;

3. Lipsa controlului centralizat și stocarea fondurilor: platformele descentralizate, fără intermediari centralizați și fără stocarea fondurilor utilizatorilor, asigură confidențialitate și securitate sporită. Această caracteristică oferă utilizatorilor protecție, dar și infractorilor oportunitatea de a efectua tranzacții discreționare, fără lăsarea de urme evidente;

4. Comunicarea și coordonarea tranzacțiilor ilegale: mixerele și exchange-urile descentralizate oferă servicii de chat între utilizatori, favorizând comunicarea și coordonarea tranzacțiilor ilegale. Acest aspect facilitează schimbul de informații despre activități suspecte și sprijină infractorii în realizarea tranzacțiilor ilegale, fără a fi detectați;

5. Implicarea platformelor în tranzacții cu cripto-active de proveniență ilicită: unele platforme de mixare și platforme descentralizate pot fi asociate cu tranzacții cu cripto-active de proveniență ilicită. Afișarea de informații sugestive pe site-ul web al platformei, precum acceptarea numerarului în tranzacții cu cripto-active sau instrucțiuni detaliate privind transferul bancar, poate indica posibila implicare în activități ilegale.

Indicatori specifici tipologiei

1. Folosirea mixerelelor: unul dintre indicatorii specifici este transferul frecvent al cripto-activelor într-un mixer, precum Tornado Cash. Infractorii pot efectua o serie de tranzacții interne și schimburi între multiple adrese diferite, astfel încât să amestece cripto-activele și să ascundă urma tranzacțiilor. Acest proces complex și repetitiv de transferuri și schimburi are ca scop îngreunarea investigațiilor și identificarea originii sau destinației fondurilor;

2. Schimbul între cripto-valute diferite: un alt indicator este schimbul cripto-activelor amestecate în alte active digitale sau în monedă fiduciară prin intermediul platformelor descentralizate. Infractorii pot folosi aceste platforme pentru a converti cripto-activele în alte forme de active, făcând urmărirea tranzacțiilor mai dificilă;

3. Lipsa verificării riguroase a identității: mixerele și platformele descentralizate nu impun măsuri stricte de verificare a identității utilizatorilor. Aceasta le permite infractorilor să deschidă conturi anonime fără a furniza informații personale detaliate sau a fi supuși unor verificări adecvate ale identității lor;

4. Mesaje sugestive privind anonimatul: acestea pot fi prezentate pe unele platforme de mixare a cripto-activelor sau pe diverse platforme descentralizate, sugerând că utilizatorii pot efectua tranzacții fără a fi detectați sau urmăriți. Aceste mesaje pot încuraja utilizatorii să aibă încredere în platformă și să considere că activitățile lor financiare vor fi ascunse și protejate de ochiul autorităților. Prin promovarea unui sentiment de anonimat și confidențialitate, aceste mesaje pot atrage atenția infractorilor care doresc să își ascundă urmele și să profite de oportunitățile de spălare de bani fără consecințe;

5. Implicarea platformelor în tranzacții ilicite: există situații în care platformele de mixare de cripto-active sau platformele descentralizate sunt implicate în tranzacții cu cripto-active de proveniență ilicită. Acest lucru poate fi evidențiat prin investigații și informații relevante despre activitățile suspecte desfășurate pe aceste platforme.

Exemple concrete:

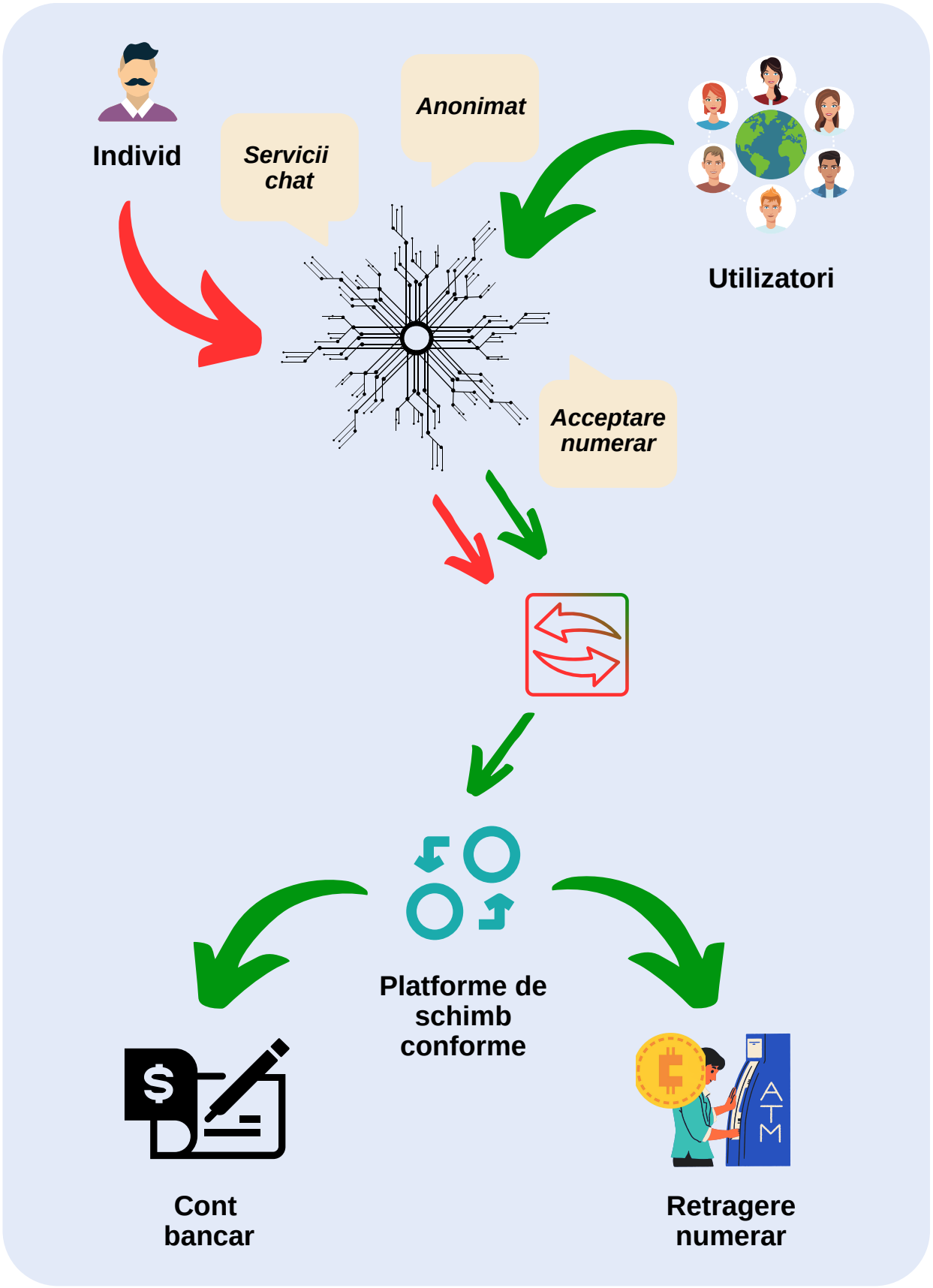
1. Silk Road a fost un marketplace online cunoscut pentru comercializarea ilegală de droguri și alte bunuri ilicite. În acest caz, utilizatorii implicați în activități ilegale au folosit mixere descentralizate pentru a amesteca cripto-activele obținute ilegal, ascunzând astfel originea fondurilor și făcându-le să pară curate.

2. AlphaBay a fost un marketplace online închis în 2017 de către FBI, cunoscut pentru vânzarea ilegală de droguri, arme și alte bunuri ilicite. În acest caz, un grup infracțional a utilizat platforma descentralizată pentru a schimba cripto-activele obținute prin activități ilegale în alte active digitale sau în monedă fiduciară;

3. Un individ sau un grup infracțional implicat în infracțiuni financiare, cum ar fi fraudă bancară sau evaziune fiscală, utilizează un mixer pentru a amesteca cripto-activele obținute prin aceste activități ilicite. Mixerul preia cripto-valutele și le amestecă cu alte fonduri provenite din surse legale, ceea ce face dificilă urmărirea și identificarea tranzacțiilor specifice.

Surse:

- United States Department of Justice (DOJ), https://www.justice.gov/usao-sdny/press-release/file/1549821/download;
- *FBI, https://www.fbi.gov/news/stories/alphabay-takedown;*
- *Europol - "Internet Organised Crime Threat Assessment (IOCTA) 2020" (https://www.europol.europa.eu/iocta-2020).*


Individ
Servicii chat
Anonimat
Utilizatori
Acceptare numerar
Platforme de schimb conforme
Cont bancar
Retragere numerar
ATM

4. Utilizarea ATM-urilor de cripto în scopul spălării banilor

În contextul creșterii popularității ATM-urilor de cripto, acestea au devenit o soluție tot mai utilizată pentru a achiziționa și a vinde criptomonede într-un mod convenabil și accesibil. Cu toate acestea, o problemă semnificativă care trebuie abordată este legată de potențialul riscului de spălare a banilor asociat cu utilizarea acestor ATM-uri.

Potrivit unui studiu* efectuat în anul 2021, România se situează pe locul 9 în lume în ceea ce privește numărul raportat de ATM-uri de cripto, având în total 86 de astfel de ATM-uri în funcțiune. Această cifră indică o prezență semnificativă a acestor facilități în țara noastră, reflectând interesul crescut al populației pentru tranzacțiile cu cripto-active și nevoia de accesibilitate la acestea. Însă, odată cu creșterea utilizării ATM-urilor de cripto, se pun în evidență și o serie de riscuri asociate, în special în ceea ce privește spălarea banilor și utilizarea necorespunzătoare a cripto-activelor.

*Sursa: https://cryptohead.io/research/crypto-ready-index

Descrierea tipologiei

Utilizarea ATM-urilor de cripto în scopul spălării banilor reprezintă o tactică eficientă prin care infractorii încearcă să transforme fondurile provenite din activități ilegale în criptomonede.

ATM-urile cripto sunt dispozitive electronice care permit utilizatorilor să cumpere și să vândă criptomonede, precum Bitcoin, Ethereum sau Litecoin, într-un mod rapid și simplu.

Prin intermediul acestui tip de ATM-uri, infractorii pot realiza tranzacții anonime și confidențiale, fără a fi nevoie să-și dezvăluie identitatea sau să treacă prin procese de verificare riguroase. Această caracteristică a ATM-urilor de cripto oferă infractorilor un mediu propice pentru a spăla banii obținuți în mod ilegal. Aceștia pot achiziționa cripto-active prin intermediul acestor dispozitive, folosind fonduri provenite din activități ilicite și apoi pot vinde sau transfera cripto-activele către alte adrese, astfel ascunzând originile și destinațiile fondurilor.

În plus, ATM-urile de cripto permit efectuarea tranzacțiilor în numerar, ceea ce face procesul de spălare a banilor și mai greu de detectat. Infractorii pot depune numerar într-un ATM de cripto și pot primi cripto-active în schimb, fără ca sursa fondurilor să fie identificată sau urmărită. Această capacitate de a converti rapid numerarul în criptomonede facilitează procesul de spălare a banilor și complică investigațiile ulterioare ale autorităților. Fiind o tehnologie relativ nouă și în continuă evoluție, regulamentele și procedurile de supraveghere pot întâmpina dificultăți în a ține pasul cu inovațiile și tacticiile utilizate de infractori.

Un alt aspect important al utilizării ATM-urilor de cripto în scopul spălării banilor este faptul că aceste dispozitive pot fi localizate în locații publice sau private, cum ar fi centre comerciale, baruri, restaurante sau chiar birouri. Acest fapt oferă infractorilor o gamă largă de locații în care pot efectua tranzacții fără a ridica suspiciuni. De asemenea, instalarea și configurarea unui ATM de cripto nu necesită licențe sau aprobări speciale în multe jurisdicții, ceea ce face dificilă monitorizarea și reglementarea eficientă a acestor facilități.

Indicatori specifici

1. Utilizarea repetată a aceluiași ATM de cripto pentru tranzacții semnificative în numerar poate ridica semne de întrebare în privința proveniență fondurilor și a scopului utilizării acestora. Aceast lucru poate indica o activitate suspectă, cum ar fi spălarea banilor sau finanțarea activităților ilegale

2. ATM-ul de cripto este amplasat în zone cu un grad ridicat de infracționalitate sau într-o locație asociată cu o afacere de fațadă, care poate fi deținută de către infractori;

3. Efectuarea unor tranzacții cu sume mari de bani într-un interval de timp scurt reprezintă o tactică utilizată pentru a fragmenta și dispersa fondurile. Scopul acestei practici este de a ascunde urmele tranzacțiilor și de a îngreuna urmărirea și investigarea ulterioară a acestora de către autorități.

4. Efectuarea tranzacțiilor prin intermediul ATM-urilor de cripto în scopul transferului rapid al fondurilor între adrese de criptomonede anonime. Utilizarea criptomonedelor cu caracter anonim facilitează ascunderea originii și destinației fondurilor, ceea ce poate indica o activitate ilegală;

5. Mai multe portofele digitale trimit fonduri prin intermediul ATM-urilor către un singur destinatar într-o perioadă scurtă de timp;

6. Utilizarea unui număr mare de carduri sau portofele digitale pentru a realiza tranzacții cu ATM-urile de cripto;

7. Efectuarea tranzacțiilor cu sume mai mici și foarte apropiate de pragurile de raportare stabilite de autoritățile financiare poate ridica suspiciuni în ceea ce privește intenția de a evita obligațiile de raportare și de a ascunde activitățile financiare;

8. Folosirea ATM-urilor de cripto în scopul transferului de criptomonede către platforme neautorizate sau neconforme din jurisdicții cu reguli slabe în ceea ce privește identificarea clientelei.

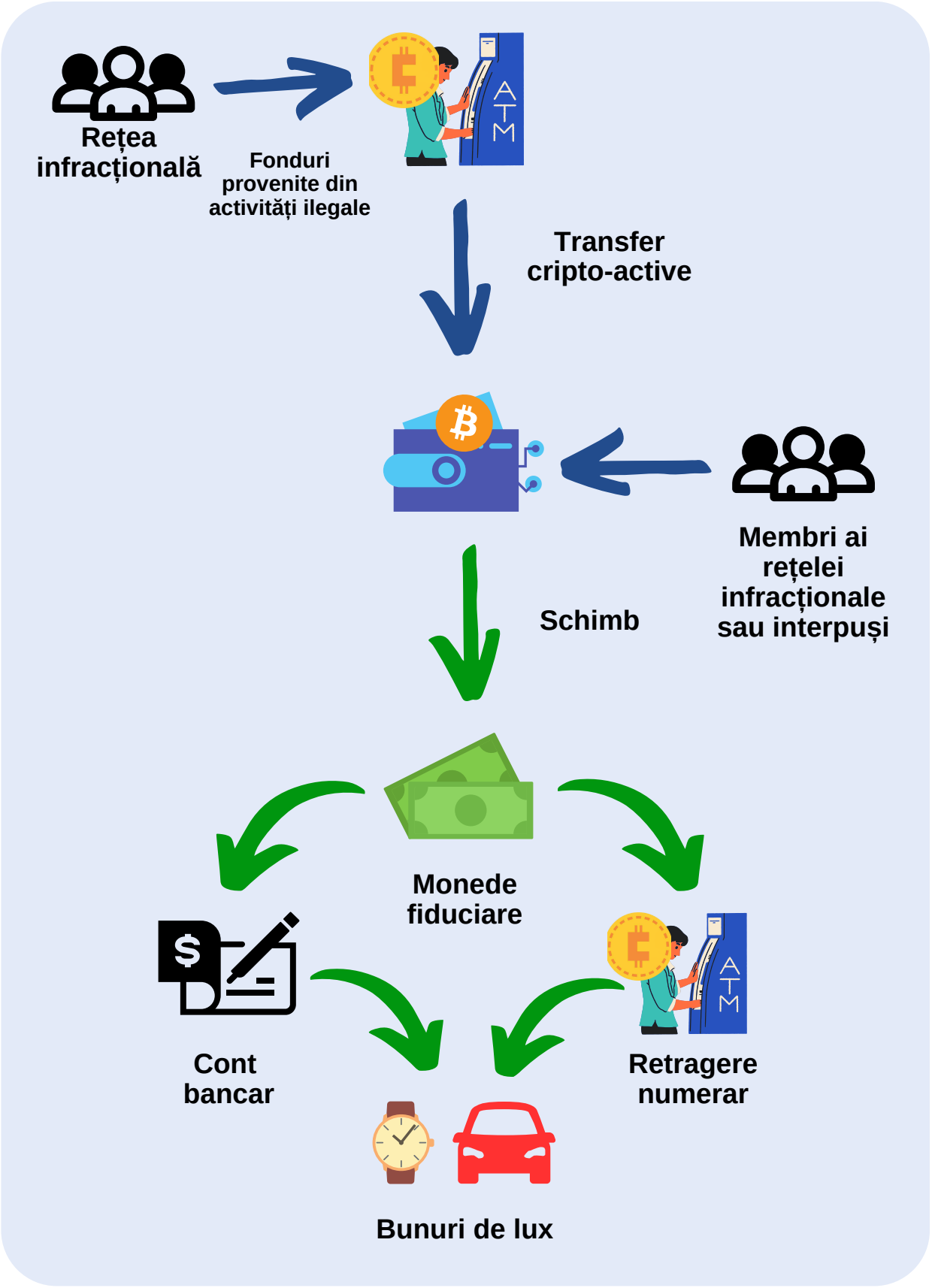
Exemple concrete

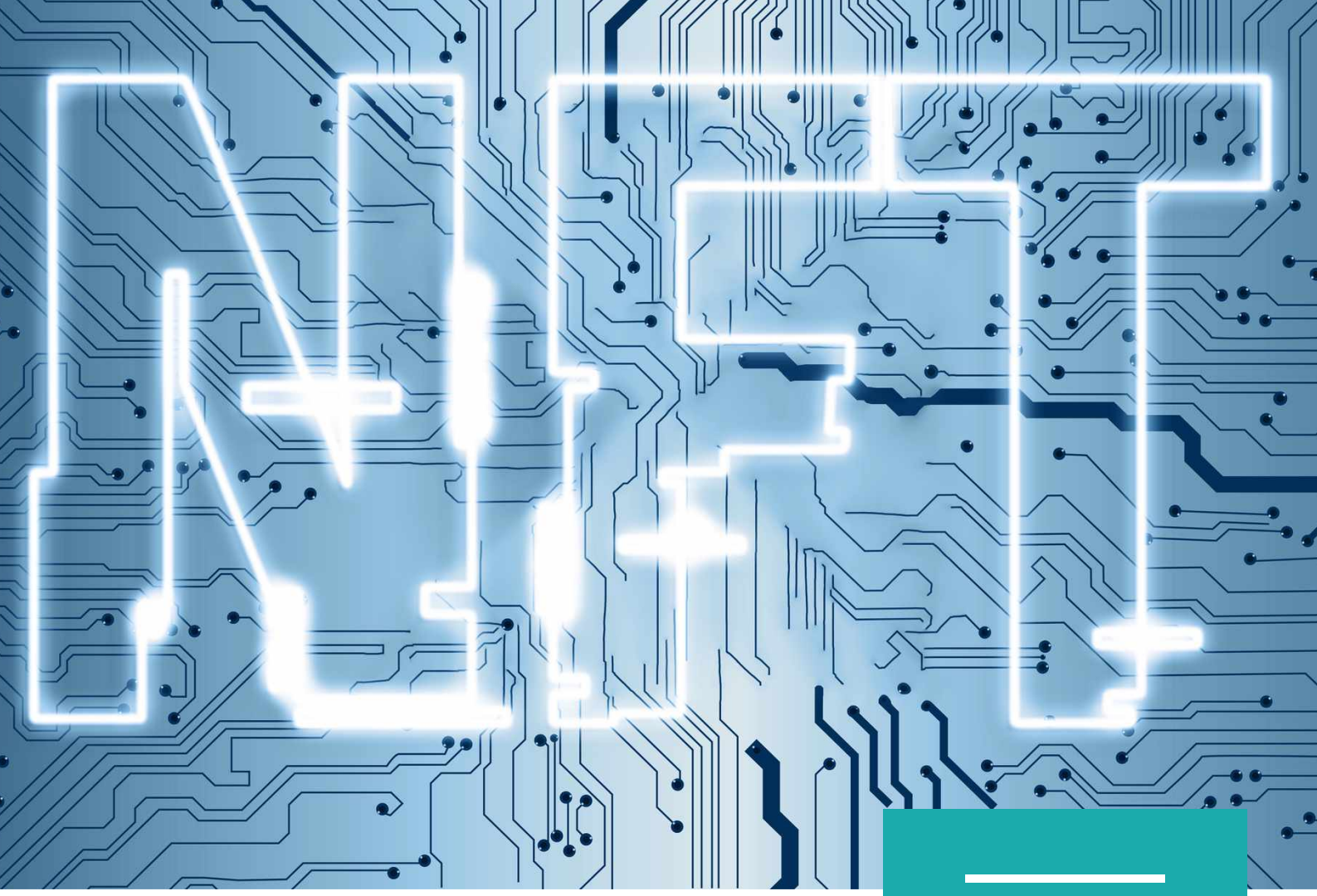
1. Un grup infracțional utilizează ATM-uri de cripto amplasate în țări cu reglementări slabe pentru a converti sume mari de bani obținute din traficul de droguri în criptomonede. Acest lucru indică o strategie adoptată de infractori pentru a ascunde și spăla fondurile provenite din activități ilegale, prin exploatarea lacunelor din reglementările și practicile de supraveghere a acestor țări;

2. Un individ efectuează tranzacții repetate de vânzare-cumpărare folosind ATM-uri de cripto. Acesta adoptă o strategie prin care fragmentează și dispersează fondurile în diferite tipuri de criptomonede, încercând astfel să îngreuneze urmărirea și investigarea tranzacțiilor sale.

Surse:

- *Elliptic Typologies Report 2022 Edition, Preventing Financial Crime in Cryptoassets;*
- *Financial Action Task Force (FATF) - Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.*


Rețea infracțională
Fonduri provenite din activități ilegale
ATM
Transfer cripto-active
Membri ai rețelei infracționale sau interpuși
Schimb
Monede fiduciare
Cont bancar
Retragere numerar
ATM
Bunuri de lux



5. Utilizarea NFT-urilor în scopul spălării banilor

NFT-urile au câștigat popularitate în ultima perioadă, reprezentând proprietatea asupra unui bun digital unic, cum ar fi o operă de artă digitală sau un joc video. Potrivit definiției dată de Clifford Change, NFT-urile sunt token-uri digitale create pe baza tehnologiei blockchain, care conferă proprietarului dreptul de a deține și tranzacționa un obiect digital unic și nedivizibil.

Cu toate acestea, o consecință nedorită a popularității NFT-urilor este utilizarea lor în scopul spălării banilor. Această creștere a utilizării NFT-urilor ridică îngrijorări semnificative în privința integrității și legalității tranzacțiilor efectuate cu acestea. Deoarece NFT-urile permit tokenizarea unor active digitale unice și chiar a unor active fizice, există riscul ca aceste tranzacții să fie folosite pentru a ascunde sau a spăla fonduri provenite din activități ilegale. Deoarece NFT-urile sunt tranzacționate online și înregistrate pe blockchain, aparenta transparență este prezentă. Totuși, datorită caracterului unic și nedivizibil al NFT-urilor, identificarea părților implicate și urmărirea originii fondurilor devin dificile.

Descrierea tipologiei

Spălarea banilor folosind NFT-urile poate implica mai multe tipuri de scheme și strategii. Iată câteva exemple ale tipologiei de spălare de bani care pot fi asociate cu NFT-urile:

1. Crearea și tranzacționarea NFT-urilor fictive: în această schemă, infractorii creează NFT-uri false sau fictive și le tranzacționează între conturile lor sau cu complicitatea unor părți terțe. Scopul este de a crea aparența unor tranzacții legitime și de a spăla fondurile provenite din activități ilegale prin intermediul acestor NFT-uri;

2. Utilizarea NFT-urilor reale, dar achiziționate cu fonduri obținute ilegal: în această strategie, infractorii utilizează fondurile obținute din activități ilegale pentru a achiziționa NFT-uri reale. Aceste NFT-uri pot fi tranzacționate ulterior pe piețele NFT legale, legitimând aparent originea fondurilor. În acest mod, infractorii încearcă să ascundă tranzacțiile ilegale și să obțină profituri "curate" prin intermediul NFT-urilor;

3. Utilizarea NFT-urilor pentru transferuri de valoare: o altă strategie de spălare a banilor prin NFT-uri implică utilizarea acestora pentru transferuri de vaoloare între diferite entități sau adrese de criptomonede. Infractorii pot achiziționa NFT-uri și le pot transfera între conturile lor sau către un complice pentru a ascunde fluxurile de bani și a îngreuna urmărirea tranzacțiilor;

4. Spălarea banilor prin intermediul artei digitale: o tactică din ce în ce mai frecventă este aceea de a asocia NFT cu arta digitală. Infractorii pot crea sau achiziționa opere de artă digitală și le pot transforma în NFT-uri, dându-le o aparență de unicitate și valoare. Aceste NFT pot fi apoi tranzacționate pe platforme NFT, iar banii din aceste tranzacții pot fi considerați "curați". Astfel, infractorii pot folosi arta digitală și NFT-urile ca instrumente de spălare a banilor.

Acestea sunt doar câteva exemple ale tipologiei de spălare de bani care pot fi asociate cu NFT-urile. Este important de menționat că aceste activități pot varia în complexitate și pot implica tehnici și strategii suplimentare pentru a ascunde tranzacțiile ilegale și a îngreuna urmărirea lor de către autorități.

Indicatori specifici

1. Tranzacții cu NFT-uri la prețuri foarte mari: tranzacțiile în care NFT-urile sunt cumpărate sau vândute la prețuri mult peste valoarea lor reală pot ridica suspiciuni cu privire la scopul ascuns al acestor tranzacții, indicând potențiala implicare în spălarea banilor;

2. Transferuri frecvente de NFT-uri între adrese anonime: astfel de transferuri poate indica un efort deliberat de a ascunde urmele tranzacțiilor și de a îngreuna urmărirea fondurilor și detectarea activităților ilegale;

3. Utilizarea platformelor de schimb neconforme sau fără licență: utilizarea unor astfel de platforme pentru tranzacționarea NFT-urilor poate indica o activitate ilegală și un mediu propice pentru spălarea banilor, deoarece aceste platforme pot oferi un grad mai mare de anonimat și o aplicare mai slabă sau inexistentă a măsurilor de conformitate;

4. Crearea de NFT-uri folosind adrese anonime reprezintă o practică în care token-urile sunt generate și tranzacționate fără a fi asociate cu identități verificabile. Aceasta poate fi realizată prin utilizarea portofelelor criptografice anonime sau a altor servicii care permit ascunderea identității utilizatorului;

5. Tranzacții cu NFT-uri în țări cu norme slabe de conformitate și reglementare reprezintă un fenomen în care aceste activități sunt efectuate în jurisdicții care au standarde reduse sau insuficiente în ceea ce privește aplicarea măsurilor de conformitate și reglementare în domeniul cripto-activelor;

6. Utilizarea NFT-urilor ca instrument pentru transferul de valoare între cripto-active reprezintă o strategie prin care se utilizează NFT-urile pentru a facilita schimbul de active digitale între diferite tipuri de criptomonede sau cripto-active.

Această utilizare a NFT-urilor poate fi exploatată în scopul spălării banilor, deoarece transferul de valoare prin intermediul NFT-urilor poate complica urmărirea fondurilor și identificarea activităților ilegale.

Exemple concrete

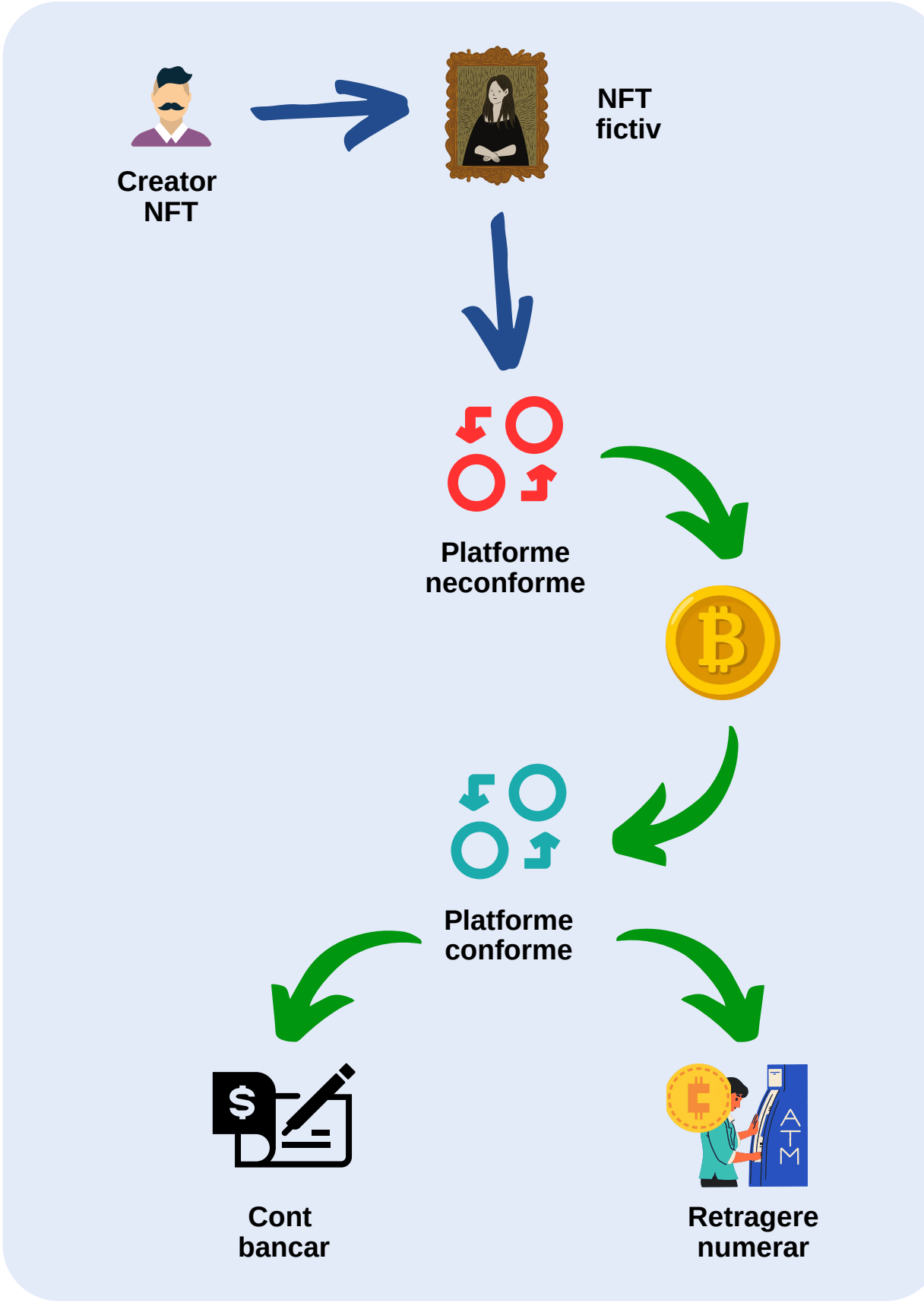
1. Un individ care deține un NFT dorește să spele o sumă de bani obținută în mod ilegal prin intermediul acestuia. Pentru a face ca NFT-ul să pară mai valoros decât este în realitate, individul creează mai multe adrese anonime în portofelul său digital. El efectuează apoi tranzacții fictive între aceste adrese, încheind cumpărări și vânzări false ale NFT-ului la prețuri exorbitante.

Prin aceste tranzacții trucate, individul reușește să creeze aparența unei cereri mari și a unui interes ridicat pentru NFT-ul său. Astfel, poate atrage atenția cumpărătorilor legitimi și să vândă NFT-ul la un preț mai mare. Suma obținută din această tranzacție este acum considerată "curată" și poate fi utilizată în mod legal, ascunzând astfel originea ilicită a fondurilor;

2. Un grup infracțional utilizează Bitcoin și NFT-uri pentru a spăla banii obținuți în mod ilegal. Datorită anonimatului oferit de blockchain, tranzacțiile cu Bitcoin sunt confidențiale și nu dezvăluie informații despre cumpărători și vânzători. Aceasta permite infractorilor să achiziționeze artă digitală sau alte active folosind fonduri obținute în mod ilegal fără a atrage atenția autorităților. Tranzacțiile cu Bitcoin sunt imutabile, ceea ce înseamnă că nu pot fi rambursate sau anulate, iar originea fondurilor rămâne necunoscută. Astfel, prin utilizarea NFT-urilor, infractorii pot ascunde proveniența ilicită a banilor și să-i legitimizeze prin intermediul tranzacțiilor aparent legale cu active digitale.

Surse:

- *Chainalysis 2022 Crypto Crime Report, https://go.chainalysis.com/2022-Crypto-Crime-Report.html;*
- *NFT money laundering and AML compliance, https://withpersona.com/blog/nfts-and-compliance-what-to-know-about-this-crypto-era-commodity.*


Creator
NFT
NFT
fictiv
Platforme
neconforme
Platforme
conforme
Cont
bancar
Retragere
numerar
ATM

6. Utilizarea ICO-urilor în scopul spălării banilor

ICO-urile (Initial Coin Offerings - Ofertă Inițială de Monede) reprezintă o metodă populară de finanțare în domeniul criptomonedelor, prin care se emite o nouă monedă digitală sau un token în schimbul investițiilor în proiecte. Cu toate acestea, utilizarea ICO-urilor poate fi susceptibilă la abuzuri și utilizare necorespunzătoare în scopul spălării banilor.

Utilizarea ICO-urilor în scopul spălării banilor reprezintă o preocupare majoră pentru autoritățile de reglementare financiară. Această practică abuzivă implică transformarea fondurilor provenite din activități ilegale în monede digitale prin intermediul ICO-urilor, cu scopul de a le integra în economia legală și de a le ascunde originea ilicită. Astfel, ICO-urile devin un instrument atractiv pentru spălarea banilor, datorită caracteristicilor lor specifice. Este important să subliniem că spălarea banilor prin intermediul ICO-urilor nu este o practică generalizată, însă este esențial să identificăm și să înțelegem riscurile asociate acestei tipologii pentru a dezvolta măsuri și soluții eficiente de combatere a acestui fenomen.

Descrierea tipologiei

1. Anonimatul: ICO-urile oferă un grad ridicat de anonimat, deoarece participanții nu sunt obligați să dezvăluie identitatea lor completă în timpul procesului de investiție. Acest lucru face ca identificarea și urmărirea tranzacțiilor să devină mai dificile, permițând spălarea banilor prin intermediul ICO-urilor;

2. Utilizarea altor criptomonede: unele ICO-uri permit investitorilor să achiziționeze token-uri folosind alte criptomonede în loc de monedele tradiționale. Acest aspect oferă oportunitatea spălării banilor prin intermediul ICO-urilor, deoarece fondurile provenite din activități ilegale pot fi mai întâi convertite într-o altă criptomonedă, apoi utilizate pentru a cumpăra token-uri în cadrul ICO-urilor;

3. Complexitatea structurilor ICO: unele ICO-uri pot avea structuri complexe și mecanisme avansate, care pot fi folosite în mod intenționat pentru a ascunde originea fondurilor și a crea un proces de spălare a banilor mai dificil de urmărit. Aceste structuri pot implica utilizarea mai multor etape de finanțare, intermediari sau adrese de criptomonede multiple pentru a complica investigațiile ulterioare;

4**. Jurisdicții cu reglementări slabe:** ICO-urile pot beneficia de jurisdicții cu reglementări slabe sau inexistente în ceea ce privește combaterea spălării banilor. Aceste jurisdicții oferă un mediu propice pentru desfășurarea ICO-urilor în scopul spălării banilor, deoarece există mai puține restricții și controale legale care să prevină și să detecteze aceste activități ilicite;

5. Utilizarea fondurilor în afara proiectelor ICO: unele ICO-uri pot fi utilizate în mod fraudulos, în sensul că fondurile strânse nu sunt folosite în mod corespunzător pentru dezvoltarea proiectului propus. În schimb, aceste fonduri pot fi direcționate în conturile personale ale emitenților sau în alte investiții speculative, contribuind astfel la spălarea banilor.

Este important de menționat faptul că descrierea tipologiei nu acoperă toate aspectele legate de utilizarea ICO-urilor în scopul spălării banilor, deoarece aceste practici pot varia în funcție de circumstanțe și strategii specifice utilizate de infractori.

Indicatori specifici

1. Volume mari de fonduri: utilizarea ICO-urilor în scopul spălării banilor poate implica investiții semnificative, deoarece sumele mari de bani pot fi fragmentate și ascunse în spatele token-urilor emise în cadrul evenimentului. Prin împărțirea sumelor mari în tranșe mici și distribuirea acestora în diferite proiecte ICO, spălătorii de bani pot obține token-uri digitale în schimbul banilor lor, ceea ce le permite să profite de potențialul de creștere al acestor active digitale și să obțină fonduri aparent legitime;

2. Utilizarea unor platforme de schimb neautorizate sau neconforme: spălătorii de bani pot alege să desfășoare ICO-uri pe platforme neautorizate sau neconforme sau în jurisdicții cu reguli slabe în ceea ce privește identificarea clientelei, pentru a evita supravegherea și verificările riguroase ale autorităților;

3. Utilizarea mixării fondurilor: spălătorii de bani pot utiliza tehnici avansate de mixare a fondurilor pentru a îngreuna urmărirea tranzacțiilor realizate în cadrul ICO-urilor și pentru a ascunde legăturile dintre adresele de criptomonede implicate. Această tactică implică amestecarea și transferul de fonduri prin mai multe adrese de criptomonede, în încercarea de a crea o rețea complexă de tranzacții care este dificil de urmărit;

4. Implicarea multiplelor jurisdicții: utilizarea ICO-urilor în scopul spălării banilor poate implica operațiuni desfășurate în diferite jurisdicții, ceea ce complică cooperarea între autorități și investigarea activităților ilegale. Spălătorii de bani pot profita de natura transfrontalieră a criptomonedelor și a ICO-urilor pentru a transfera fonduri între diferite țări și jurisdicții cu reguli diferite privind criptomonedele și spălarea banilor;

5. Complexitatea tranzacțiilor: utilizarea ICO-urilor în scopul spălării banilor implică adesea transferuri de fonduri între adrese de criptomonede anonime, utilizând tehnici avansate de criptografie și protocoale blockchain complexe. Această complexitate a tranzacțiilor face dificilă urmărirea fluxurilor de bani și identificarea originii acestora.

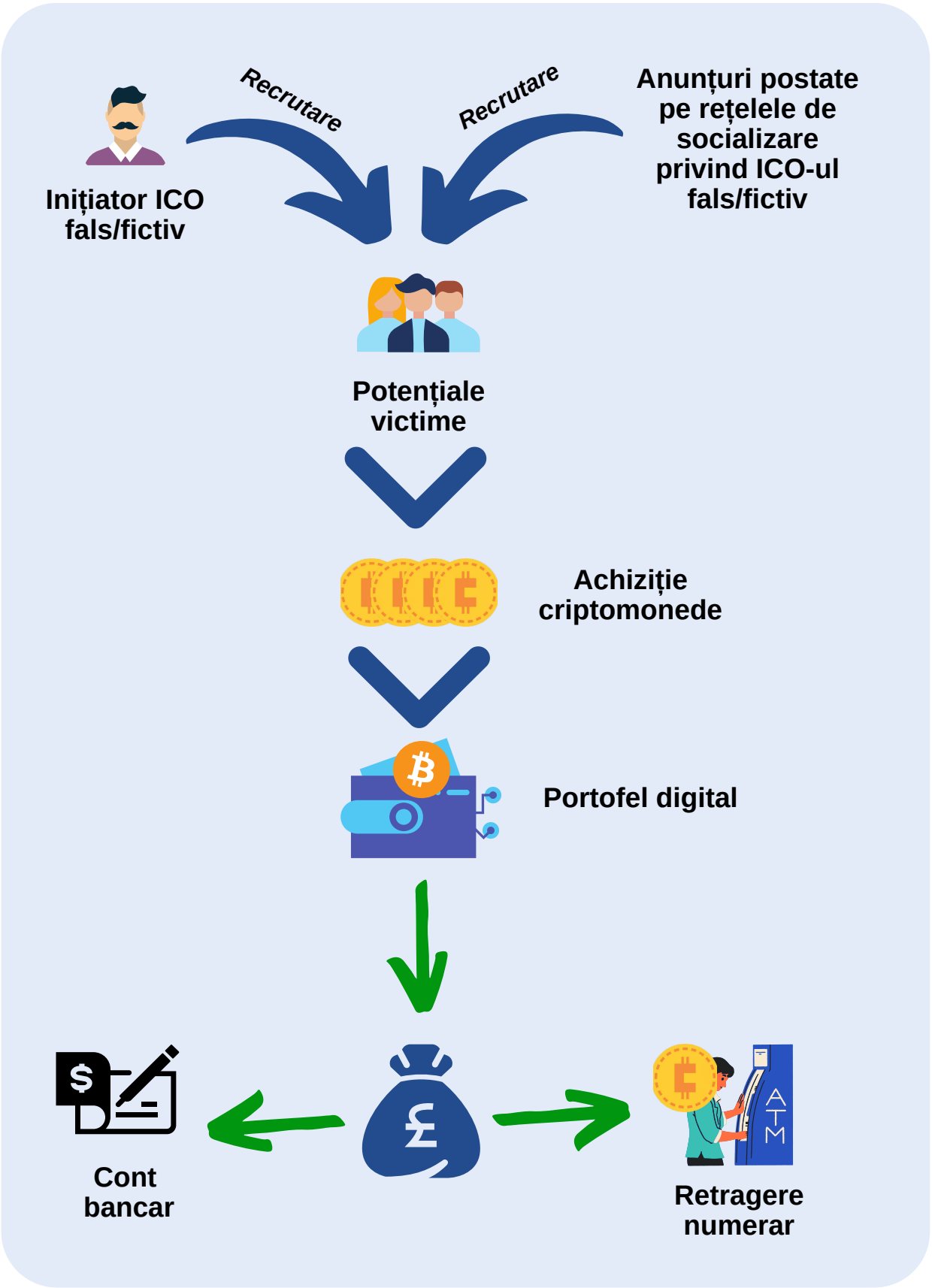
Exemple concrete

1. Utilizarea unor platforme neautorizate sau neconforme: în perioada 2017-2020, Comisia pentru Bursă și Valori Mobiliare a SUA (SEC) a emis avertismente și a intentat acțiuni legale împotriva mai multor ICO-uri care au fost identificate ca fiind neautorizate și care nu respectau reglementările privind valorile mobiliare. Aceste acțiuni legale au vizat încercările de spălare a banilor prin intermediul ICO-urilor și au avut ca rezultat sancțiuni financiare și interdicții. SEC a intentat acuzații împotriva lui Dominic Lacroix și companiei sale, PlexCorps, pentru că au promovat și vândut valori mobiliare numite PlexCoin pe internet către investitori din SUA și din alte țări. Aceștia au făcut afirmații false, susținând că investițiile în PlexCoin ar aduce un profit de 1.354% în mai puțin de 29 de zile;

2. Utilizarea mixării fondurilor în cadrul ICO-urilor poate fi exemplificată prin proiectul platformei de criptomonede Monero. În cadrul procesului ICO, Monero a implementat tehnici avansate de mixare a fondurilor pentru a îmbunătăți nivelul de confidențialitate al tranzacțiilor. Acest lucru a fost realizat prin utilizarea unui protocol special denumit "Ring Confidential Transactions". Acest protocol grupează tranzacțiile într-un "inel" de semnături digitale, ceea ce face dificilă identificarea originii tranzacțiilor. Această practică a atras atât investitorii preocupați de confidențialitate, cât și indivizi cu intenții ilegale, care au văzut în Monero o modalitate de spălare a banilor. Amestecul de fonduri a sporit opacitatea și a îngreunat investigarea tranzacțiilor suspecte de către autorități.

Surse:

Comisia pentru Bursă și Valori Mobiliare a SUA, SEC Emergency Action Halts ICO Scam, https://www.sec.gov/news/press-release/2017-219;
Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing, https://ciphertrace.com/virtual-asset-red-flag-indicators-of-money-laundering


Recrutare
Recrutare
Anunțuri postate pe rețelele de socializare privind ICO-ul fals/fictiv
Inițiator ICO fals/fictiv
Potențiale victime
Achiziție criptomonede
Portofel digital
Cont bancar
Retragere numerar

V

Concluzii

Acest raport complex elaborat de către Oficiul Național de Prevenire și Combatere a Spălării Banilor a analizat în detaliu problema spălării banilor în domeniul cripto-activelor. Fenomenul reprezintă o provocare semnificativă pentru instituțiile financiare, autoritățile de reglementare și organizațiile din domeniul cripto-activelor.

Pe parcursul studiului, am constatat că spălarea banilor în acest domeniu reprezintă o provocare semnificativă din cauza caracteristicilor specifice ale cripto-activelor, precum anonimitatea și descentralizarea. Aceste aspecte facilitează ascunderea originii fondurilor ilicite și dificultățile în urmărirea acestora de către autorități. Prin urmare, este imperativ ca toate părțile implicate să colaboreze pentru a dezvolta soluții eficiente în combaterea acestui fenomen.

Colaborarea între instituțiile financiare tradiționale și platformele de cripto-active este deosebit de importantă în acest context. Integrarea unor sisteme eficiente de monitorizare și raportare a tranzacțiilor suspecte, precum și implementarea unor măsuri riguroase de verificare a identității utilizatorilor pot contribui semnificativ la prevenirea și combaterea spălării de bani în acest domeniu.

De asemenea, cooperarea internațională între autoritățile de reglementare și organizațiile specializate în combaterea criminalității financiare este esențială pentru a face față acestui fenomen transfrontalier. Schimbul de informații și bune practici, precum și coordonarea investigațiilor și aplicarea legii, pot spori eficiența în identificarea și urmărirea infractorilor implicați în spălarea de bani.

Constatăm că utilizarea platformelor neconforme și a mixerelor facilitează spălarea de bani prin transferul și amestecul cripto-activelor, ascunzând astfel originea și urma tranzacțiilor. Aceasta reprezintă o provocare majoră pentru autoritățile de reglementare și aplicare a legii, deoarece implică un grad ridicat de anonimat și dificultăți în urmărirea activităților ilegale.

Pentru a trata această problemă, este necesară o abordare integrată, care să combine reglementările și măsurile de conformitate cu educația și conștientizarea utilizatorilor de cripto-active. Încurajarea unui mediu sigur și responsabil, în care utilizatorii sunt informați cu privire la riscuri și obligații, joacă un rol crucial în prevenirea și reducerea fenomenului de spălare de bani în acest domeniu.

De asemenea, este important ca platformele de cripto-active să adopte măsuri riguroase de verificare a identității utilizatorilor, să monitorizeze tranzacțiile suspecte și să colaboreze strâns cu autoritățile de reglementare și aplicare a legii pentru a identifica și opri activitățile ilicite, în acest fel își protejându-și integritatea și reputația.

Oficiul Național de Prevenire și Combatere a Spălării Banilor se angajează să continue eforturile în dezvoltarea unui cadru legal adecvat și în promovarea unei cooperări eficiente între toate părțile implicate pentru combaterea spălării de bani în mediul cripto-activelor.

Autori:

Mihai MEHEDINȚU - Analist Financiar, Direcția Prevenire, Supraveghere și Control, Compartimentul Supraveghere și Instruire Cripto-Active

Irina Anca GEORGESCU - Șef Compartiment Evaluarea Națională a Riscurilor, Analiza Strategică și Metodologie, Direcţia Tehnologia Informației, Baze de Date şi Statistică

București,

Iunie 2023